Issue 1

FastAccess NMS Requirements

ii

Contents

vi

List of Figures

ix

List of Tables

xii

1. Introduction

This document provides an initial set of requirements for the proposed FastAccess (internally also called PC/DNA) Network Management System (NMS) in the time frame. This NMS will be integrated into an operations environment that is described in the FastAccess Operations Technical Plan (OTP) [1].

Two releases of the NMS are expected in 1998 – Release 1 is targeted for and Release 2 is targeted for It is envisioned that the infrastructure provided by this system will evolve to provide a general purpose broadband operations system supporting ATM and other services. Hence, the NMS, at its evolution, will not be specific to the FastAccess service.

It is expected the Release 1 requirements specified in this document will be baselined by all major stakeholders representing FastAccess project management, FastAccess Operations SME team, Work Center user (i.e., DCSC), S&T requirements, and development teams.

1.1 Purpose and Scope

This document addresses FastAccess NMS application requirements, system-to-system interface requirements, and system level requirements.

For Release 1 of NMS, the existing system-to-system interfaces will be used as they are, without any enhancement (exception: the SOCS/NMS interface needs to be defined and developed). Hence, the existing interface documents are referenced and used as appropriate. For Release 2, the enhancements to these interfaces will be specified and negotiated.

Since the platform to implement the FastAccess NMS is already selected to be the OSI NetExpert, the system level requirements are within the scope of the existing capabilities of this platform.

Although this document addresses the user interface functional requirements to perform certain operations tasks, it does not provide user screen design requirements nor does it describe how the GUI should look. Consistent with these requirements, the GUI design and flow are covered in a separate document [10].

This document describes a set of features, designated as NMS R1 or NMS R2 features. Some features are also designated as (O), which means "Objective" for NMS R1. Each of these features is described according to the following outline:

⇒ "Purpose of the feature" – provides a high-level motivation for developing the feature

⇒ "Dependencies of the feature" – itemizes other features that are required for implementing this feature
⇒ "Flow of the feature" – outlines the flow of the functions and messages
⇒ "Feature requirements" – conveys the formal requirements
⇒ "Issues/Questions" – lists a set of outstanding issues and questions.

1.2 Notation

- FastAccess is the marketing name for PC/DNA.
- Network Service Provider (NSP) is used to mean either an Internet Service Provider (ISP) or a Corporate LAN.
- The term PVC as used in this document is an end-to-end ATM entity. It may be either a Virtual Channel Connection (VCC) or a Virtual Path Connection (VPC). Each end-to-end PVC is identified in NMS by a unique PVC ID.
- From the NMS perspective, the ATM network (which is implemented by the Ascend switches) is a subnetwork. A connection across the ATM subnetwork is called a "subnetwork connection."
- The "Service Gateway" is a network element that provides the service gateway functions, including authentication and session management, and plays a role of proxy agent to the NSP Router. An initial implementation of the Service Gateway will use the Alcatel equipment called DANA/SMC.
- All requirements specified in this document are NMS Release 1 requirements, unless specified as "O," which indicates an objective for Release 1. Some NMS R2 requirements are also specified.

1.3 Document Road Map

This document is organized as follows:

⇒ Section 2 describes the "NMS Operations Environment and Assumptions."
⇒ Section 3 addresses the "NMS Generic Requirements."
⇒ Section 4 focuses on the "Network Creation Requirements."
⇒ Section 5 describes "Capacity and Inventory Management Requirements."
⇒ Section 6 addresses the "Service Order Management Requirements."
⇒ Section 7 focuses on "PVC Management Requirements."
⇒ Section 8 discusses the "Fault Management Requirements."
⇒ Section 9 describes the "Performance Management Requirements."
⇒ Section 10 addresses the "Security Management Requirements."
⇒ Section 11 addresses the "NMS External Requirements."
⇒ Section 12 lists "Open Issues and Questions."
⇒ Section 13 provides "Acknowledgments."
⇒ Glossary
⇒ References lists the publications cited in this document.

1.4 Authors and Contributors

The authors for this document are Maureen Juneau, S.K. Malhotra, Shawn Shokoohi (Editor), Grace Wrigley, and Joe Xavier. Also, Jim Hodge and Phiroz Madon provided substantial contributions to the initial two drafts.

1-4

2. NMS Operations Environment and Assumptions

This section describes NMS operations environment and provides a list of assumptions.

2.1 The NMS Operations Environment

This section describes the FastAccess network architecture, NMS operations environment, and a high-level view of the NMS features.

2.1.1 FastAccess Network Architecture

Figure 2-1 depicts the network architecture for the FastAccess service. It consists of Digital Subscriber Line Access Multiplexers (DSLAMs), the ATM subnetwork, and the Service Gateways (SG). It is assumed that each DSLAM is logically connected to only one SG via a VPC. Note that the network element called Bridge/Mux in the OTP [1], is now replaced by a "Service Gateway" that provides proxy and session management functionalities to multiple ISPs and Corporate LANs. Initially, the SG concept will use the Alcatel equipment, called DANA/SMC.

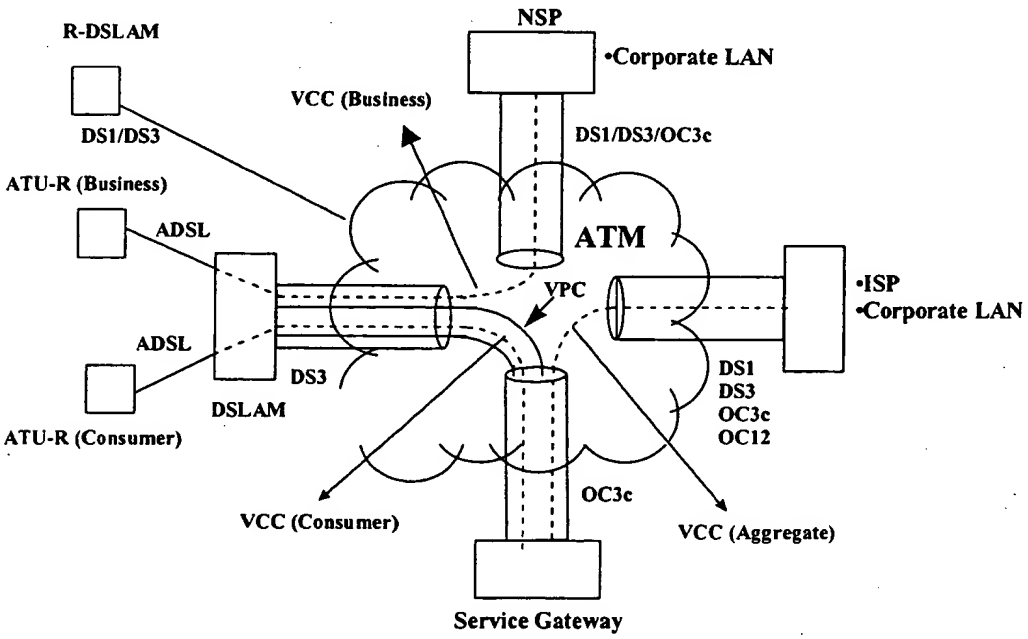

Figure 2-1. Network Architecture for the FastAccess Business and Consumer Services

As Figure 2-1 depicts, it is assumed that both classes of services, consumer/residential class (best effort/no guarantees) and business class, are supported. The high-end business class that specifies a minimum bandwidth requires provisioning of a VCC from ATU-R to the Corporate LAN or ISP without going through the SG. The residential service requires provisioning of a VCC from ATU-R to the SG, while going through the pre-provisioned VPC between the DSLAM and SG.

2.1.2 FastAccess Service Description

Two classes of service are proposed for time frame [11]-consumer class and business classs.

2.1.2.1 Consumer Class FastAccess ADSL

This is a "best effort" category 1 class of service, which is non-designed and uses the SG (also called residential class). For each consumer, a VCC will be configured from ATU-R to the appropriate SG. Through the SG, the customer will have access to one or more providers (ISPs or Corporate LANs).

The downstream bandwidth is 256 kbps to a maximum of 1.0 Mbps "throttled" at the DSLAM via the ADSL profile. The upstream bandwidth is 128 kbps.

2.1.2.2 Business Class FastAccess ADSL

Two variations of business-class services will be supported:

- Best-effort - No Guarantees (low end business service)
- Designed - Minimum Bandwidth Guarantees (high end business service).

The "best-effort/no guarantees" category 2 is the business version of the consumer class (i.e., non-designed) that uses the SG. The only difference is that the upstream bandwidth is 384 kbps (rather than 128 kbps).

The "minimum bandwidth guarantees" category 3 is a direct connect ATM service from ATU-R to the NSP (ISP or Corporate LAN) without going through the SG. This service may or may not be a "TIRKS® " designed service. There will be three tiers of the service with guarantees at each tier [11]:

1) Downstream speed of 256 kbps to 1.5 Mbps - throttled at a maximum of 1.5 Mbps
2) Downstream speed of 1.5 Mbps to 3.0 Mbps - with guaranteed minimum bandwidth of 1.5 Mbps and throttled at a maximum of 3.0 Mbps
3) Downstream speed at 3.0 Mbps and higher - with guaranteed minimum bandwidth of 3.0 Mbps.

TIRKS is a registered trademark of Bellcore.

2-2

The upstream speed for all the above three tiers will be 384 kbps and higher.
Question: For the "minimum bandwidth guarantees" 3 tier services, is the throttling done at the ATM layer?
Remark: For Release 1, it is assumed that all flow-through service orders (business and consumer) will only come through SOCS. If there is any service order that is TIRKS designed, it will have to be provisioned via the NMS GUI and will not flow-through. For TIRKS designed services, an interface to NSDB will be considered in future.

2.1.3 The Need for NMS

The FastAccess OTP [1] has established the need for end-to-end management of ATM logical entities across the multiple EMSs. Currently, such functionalities are not provided by any existing system. The legacy systems manage the physical entities only. The vendor EMSs while managing that specific vendor subnetwork, do not provide for end-to-end management of the PVCs across multiple EMSs. The NMS, specified in this document, will fill the gap by providing the end-to-end management of PVCs and by providing a single user interface across multiple vendors EMSs. This will obviate the need for accessing multiple EMSs to perform certain end-to-end operations tasks as it is done today in the Birmingham trial.

Figure 2-2 indicates three types of EMSs that are anticipated to be deployed to support the FastAccess service in the time frame. They are Alcatel's AWS, Ascend's NavisCore (formerly called CascadeView), and a Service Gateway EMS (to be developed). As Figure 2-2 indicates, it is anticipated that other EMSs will also evolve to support alternative architectures associated with the FastAccess service in time frame. They are related to Lucent and NORTEL integrated ADSL solution, Pulsecom Mini-RAM, and RTEC NGDLC integrated ADSL solution.

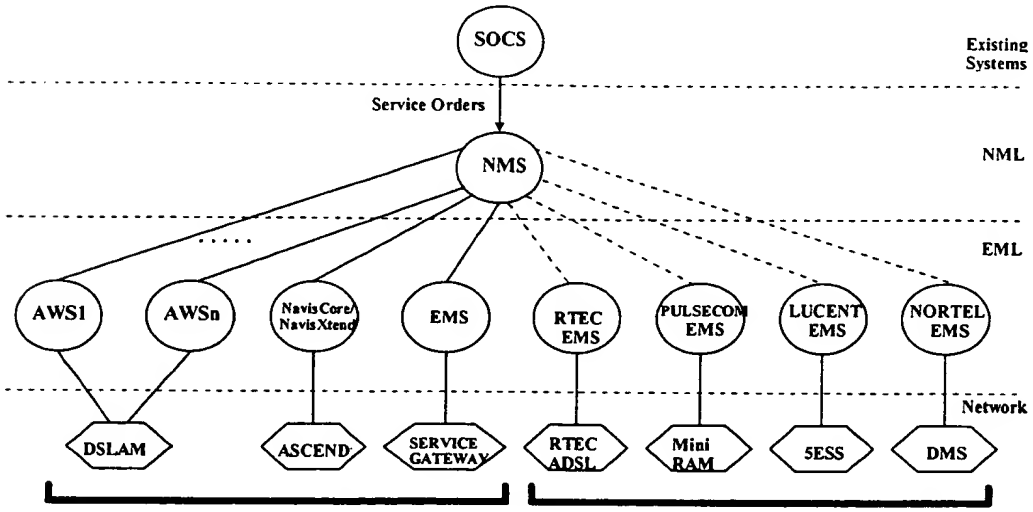

Figure 2-2. Single User Interface Across Existing and Evolving EMSs

While the initial thrust of the NMS is to focus on management of the FastAccess service, it is anticipated that this system will evolve to a service independent system and will become a general purpose "Broadband NMS" supporting ATM, Frame Relay, and other services. Hence, it is expected that the infrastructure provided in the initial release of the NMS to support the FastAccess service will provide the foundation to support other services.

2.1.4 NMS Operations Environment

The NMS operations environment is described in the FastAccess OTP [1]. The requirements described in this document are, for the most part, based on the operations processes described in that OTP.

For the ; time frame, project management has decided that DCSC will evolve to perform the BBOC [1] functionalities for FastAccess service. The Help/Service Center functions will be outsourced and a vendor will be selected after evaluating responses to the BellSouth RFP. In the Birmingham trail, Telemon is performing the Help/Service Center functions.

In addition to DCSC, the NMS may also have other users such as the FastAccess Help/Service Center [1] and Capacity Planning Centers responsible for capacity planning

for DSLAMs. The Help/Service Center, which is "customer facing," may have limited NMS access (mostly passive/read-only) for checking the network status and identifying network failure impact on individual customers.

Figure 2-3 provides the operations environment for NMS Release 1. The NMS will interface to Alcatel's AWS (a pass-through interface) and to two of the Ascend's NavisXtend Servers called Provisioning Server (PS) and Fault Server (FS). These servers provide APIs, command line, and SNMP interfaces. The provisioning server enables NMS to provision a "subnetwork connection" across the Ascend ATM subnetwork. The fault server enables the NMS to receive the FastAccess related service impacting ATM alarms.

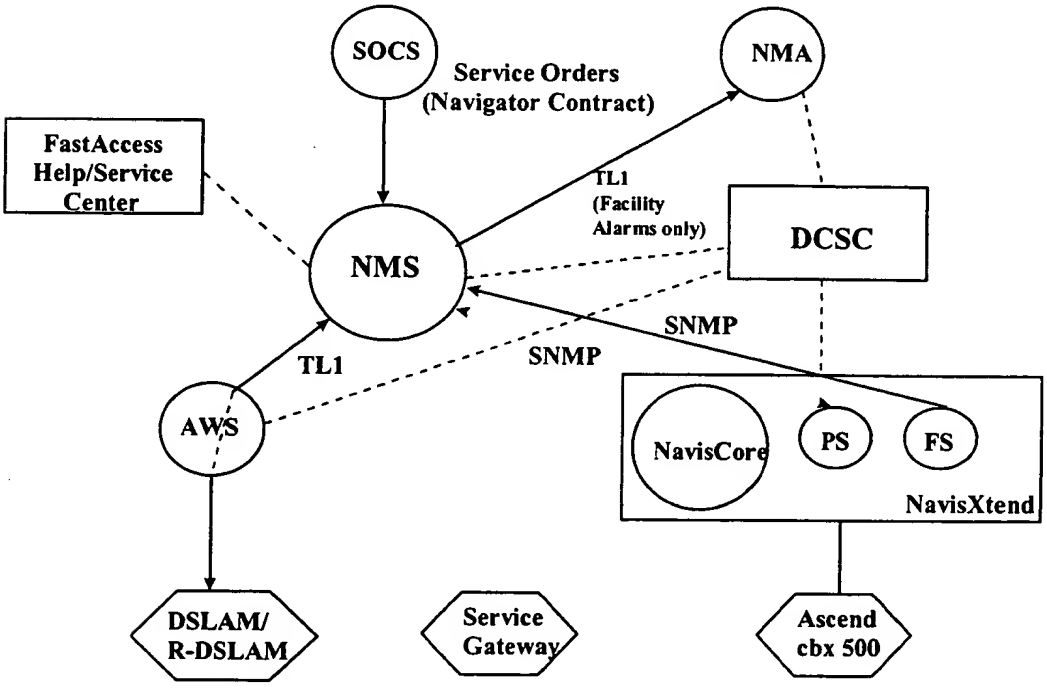

Figure 2-3. The NMS Operations Environment for Release 1

Another NMS interface is an interface to SOCS to receive the FastAccess residential and business service orders for flow-through provisioning.

The NMS will monitor all FastAccess impacting alarms & alerts. The NMS will forward a subset of these alarms, namely, the facility alarms (i.e., DS1/DS3/OC3 alarms), to

NMA and NRC (Network Reliability Center) for NMA alarm correlation. *The delivery of alarms to NMA is subject to Alcatel and Bellcore performing the appropriate OSMINE functions for AWS TL1 interface.* It is assumed that the DCSC will be provided with an NMA terminal [1] to use the NMA alarm correlation capability. This capability will prevent DCSC from initiating any unnecessary maintenance activities that are due to the higher level facility failures in the network (e.g., OC12 or OC48 failures).

A totality of NMS and associated EMSs functions will be available to the DCSC user from a single NMS terminal. To accommodate this capability, a "cut-through" function from the NMS to all subtending EMSs, including AWSs and NavisCore, will be supported.

It is assumed that the installation and provisioning of the physical equipment are to be performed by the EMSs. The NMS will focus on "end-to-end" and "cross-EMS" management of logical entities such as ATM VCCs and VPCs. The NMS will provide a complete network topology view including DSLAMs, Service Gateways, and relevant edge switches/ports of the ATM subnetwork. This is necessary for managing "end-to-end" entities. The NMS will provide some aspects of customer/service data.

The initial installation of DSLAMs may be performed by an NMS user who could "cut-through" to the specific AWS GUI and perform the required provisioning functions. The installation and provisioning of the ATM switches, SONET, and DS3/DS1 facilities in the backbone ATM network will be performed by Ascend's NavisCore (formerly called CascadeView).

NMS Release 1 will be integrated in an operations environment with the following system-to-system interfaces:

- ⇒ TL1 interface to AWSs to manage DSLAMs
- ⇒ SNMP (or API/command line) interface to NavisXtend Provisioning Server to provision a "subnetwork connection" across the ATM subnetwork
- ⇒ SNMP interface to NavisXtend Fault Servers to receive FastAccess related failure notifications
- ⇒ TL1 interface to NMA to forward the DSLAM facility (DS1, DS3, and OC3) alarms to NMA for alarm correlation
- ⇒ "Navigator Contract" interface to obtain SOCS service orders for flow-through service activation. *If the SOCS/NMS system-to-system interface will not be available by (i.e., in time for Release 1 of NMS), an "electronic transfer" of SOCS service orders to NMS will be supported.*

Note: Although the NavisCore supports "subnetwork" management functionalities, since it only supports one vendor network element, it is considered to be an Element Management System (EMS) and not a Network Management System (NMS).

2.1.5 High-Level View of the NMS Functions

The NMS functions are discussed in detail in the subsequent sections. At a high level, the NMS will provide the following functions:

- ⇒ *"Cut-through"* capability to access all EMS GUIs from the NMS workstation.
- ⇒ User capability to *"create"* all the appropriate network entities in the NMS database. It is assumed that actual installation of the network elements (e.g., DSLAM, SG, ATM switches) and physical facilities are performed via EMSs and not NMS.
- ⇒ *"Capacity and inventory management."* NMS will provide user-selectable capacity thresholds for DSLAMs. If these thresholds are crossed, autonomous alerts/reports will be issued by the NMS. The NMS user will also have on-demand and periodic capability to retrieve DSLAM capacity and inventory information.
- ⇒ Capability to *"automatically provision a PVC"* across the AWS and NavisCore from ATU-R to a Service Gateway or directly to a NSP. This capability may be performed in a flow-through manner by obtaining the FastAccess service orders from the SOCS or via the NMS GUI. Other types of PVCs that are not FastAccess service order driven (i.e., a VPC from DSLAM to SG or a VCC from SG to ISP) may also be provisioned via the NMS GUI. The ADSL and ATM parameter profiles will also be provisioned as an integral part of the PVC provisioning process. There will be a PVC ID associated with all end-to-end PVCs (i.e., any VCC or VPC).
- ⇒ *"Fault Management."* NMS will receive ADSL, ATM, PVC, customer port, equipment, and facility alarms from AWS and NavisXtend fault server. It will correlate the alarms for user presentation and will forward a subset of those alarms to NMA (facility alarms only). The NMS will provide alerts for all NMS detected failures (e.g., PVC provisioning failures).
- ⇒ *"Diagnostics."* Upon entry of a customer ID (i.e., TN) or a PVC ID by the NMS user, all network resources (physical and logical) related to that PVC will be provided.
- ⇒ *"Customer data."* By parsing the SOCS service order information or by manual entry, the NMS shall provide a limited set of customer data.

2.2 Philosophy & Assumptions

2.2.1 General Service Assumptions

1) Both consumer (or residential) and business classes of service will be supported by each DSLAM (Figure 2-1). The consumer class and "best effort" business classes use the Service Gateway to connect to an ISP or to a corporate LAN. For these services, a PVC will be provisioned from ATU-R to the Service Gateway. The "minimum bandwidth guarantee" business class does not go through the

Service Gateway. In this case, an end-to-end PVC will be provisioned from the ATU-R to Corporate LAN or ISP.

2) When the Service Gateway is used, only one PVC per customer is assumed.
3) It is assumed that physical links (DS1/DS3/OC3/OC12) have already been provisioned between the NSP and the BellSouth ATM switch (Figure 2-1). This link may be used for multiple services and is "not" dedicated to the FastAccess service. Other physical links (OC3) must also be provisioned between the Service Gateway and ATM switch. These physical links and their Circuit IDs (CIDs) will be entered in NMS database when creating those links in the NMS.

2.2.2 Consumer Service Assumptions

1) It is assumed that VCCs (big pipes) are already provisioned from the Service Gateway to the ISPs and Corporate LANs (this is part of the resource provisioning). It is noted that although there is no FastAccess service order associated with such VCCs, there may be an ATM service order. The trigger for the NMS user to provision such VCCs must be specified as a part of the DCSC M&Ps.
2) Each DSLAM is logically connected to *one* Service Gateway via a VPC (Figure 2-1). There is no FastAccess service orders for these VPCs (there may be an ATM service order). The DCSC M&Ps must specify the trigger for NMS user to provision these VPCs.
3) The consumer service is viewed as an access to the Service Gateway. To provide an end-to-end service, it is assumed that the Service Gateway will ensure connectivity of the customers to the specific ISP of their choice. The customer may specify selected NSPs at the time of service negotiation with CSA. The CSA needs to verify that the customer selected NSPs are supported by that customer serving DSLAM. The NMS must check to verify that the customer selected NSPs are supported by the specific Service Gateway.
4) The DCSC does not need to inform an NSP when a customer VCC from ATU-R to the Service Gateway is provisioned.
5) The NMS does not keep track of customer sessions with various NSPs.

2.2.3 Business Service Assumptions

The business customer service order is initiated by the NSP Administrator rather than the end user. The NSP Administrator will specify the physical circuit ID for the link between the NSP and ATM switch, associated VPI/VCI and bandwidth tier of the ADSL.

2.2.4 Network Assumptions

1) The Remote DSLAMs (R-DSLAMs) will be connected directly to the ATM switch. That is, R-DSLAMs are "not" subtending to the CO DSLAMs. Hence, from the NMS perspective, R-DSLAM will be treated similar to the CO DSLAMs

and a VPC will be provisioned between R-DSLAM and the Service Gateway. It is assumed that R-DSLAM is a hardened version of a CO DSLAM and they are identical otherwise.

2) The service orders from the SOCS must distinguish between CO DSLAM and R-DSLAM. The R-DSLAM port assignment in the SOCS service orders will have the LFACS naming convention for the cable and pair. The CO-DSLAM port assignment in the SOCS service orders will have the COSMOS naming convention.
3) Alcatel and Pulsecom Mini RAMs (i.e., Pizza Box) will be available sometime in late Hence, no support for these network elements will be provided in Release 1 of NMS.
4) The Service Gateway will not be physically connected to DSLAMs. The DSLAM OC3/DS3 interface is directly connected to the Ascend ATM switches. The DSLAMs and Service Gateways are logically connected via a VPC. It is initially assumed that each DSLAM is connected to only one Service Gateway.
5) For Release 1, use of ADSL R3.0, Cascade provisioning server (R 2.0) and Cascade fault server (R1.0) are assumed.

2.2.5 General Operations Assumptions

1) The OTP [1] forms the foundation for the FastAccess operations architecture. Specifically, it is assumed that the ADSL equipment will follow the "POTS flow" rather than "special services flow." The POTS flow applies to low-end business (best effort) as well as consumer classes of service. The high-end business class (minimum bandwidth guarantee) may or may not follow the "special services or TIRKS designed flow" (this issue will be addressed by the SME Team). All other non-ADSL elements of the FastAccess network will follow the special services flow i.e., TIRKS flow.
2) Release 1 of NMS *will not* support flow-through service activation for the special services or TIRKS designed flow. That is, no automated interface from NSDB to NMS to obtain the WORD document will be provided. If the FastAccess business services follow the special services flow, then the PVC may be implemented using the NMS GUI.
3) For Release 1, the existing EMS interfaces will be used as they are and no enhancement of these interfaces will be assumed. That is, the TL1 interface provided by ADSL 2.3 and 3.0, the SNMP interface supported by the Release 2 of Ascend Provisioning Server and the SNMP interface supported by the Release 1 of Ascend Fault Server will be used.
4) Due to lack of required information on the Service Gateway (SG), its interfaces, and associated EMS, no active management of the SG will be provided in Release 1 of the NMS. Hence, Release 1 will concentrate on well known and stable ATM/ADSL entities such as DSLAM/AWS and Ascend provisioning and fault servers. However, the SG will be created in the NMS database, and NMS users will be provided with the "cut-through" capability to the SG via the NMS

workstation. The IP management issues pertaining to the SG will be addressed in the subsequent releases of the NMS.

5) The customer ID is assumed to be the TN.
6) For PVC assignment there will be no bandwidth capacity considerations when using the POTS flow.

2.2.6 SOCS Interface Assumptions

1) *It is expected that the SOCS interface will be available by . in order to be included in Release 1 of NMS.* If the interface is not available in the required time frame, an "electronic" or "terminal emulation" interface will be provided to avoid manual order entry into the NMS.
2) All the SOCS service orders received by NMS will include a DSLAM port assignment with appropriate COSMOS or LFACS naming convention.
3) To simplify SOCS requirements, the screening of the SOCS service orders will be done in NMS, i.e., NMS will screen out the information in the SO that it does not need, e.g., billing information.
4) Initially only "new connect," certain type of change orders, and "disconnect" service orders will be supported. The "change orders" that reflect change to a completed service will be RMAed and will need to be processed manually via the NMS GUI.
5) For consumer and low-end business (i.e., best effort) customers that use the Service Gateway, the following information must be included in the SOCS service orders: type of service order, type of service, due date, serving DSLAM, DSLAM port assignment (presented in either COSMOS or LFACS naming conventions), and list of NSPs requested by the consumer.
6) For the high-end business service orders in addition to the above information, the following additional information is required in the SOCS service order: 1) the Circuit ID identifying the specific physical facility between NSP and ATM switch (Figure 2-1), 2) the range of VPI/VCIs or specific VPI/VCI for that specific Circuit ID, 3) Optional NSP provides ID/name for the end-to-end VCC from ATU-R to NSP.
7) In Release 1 of NMS, the third-party ATU-R installer will report the completion to MSOC/CAT (which subsequently will update SOCS), as it is done today. Upon completion, SOCS will notify NMS of completed status of the service order.
8) In Release 1, the communications with SOCS will be "one way," from SOCS to NMS (the only exception may be NMS acknowledgment of receipt of service orders) . In subsequent releases, when the auto-discovery feature is available, the NMS may automatically discover ATU-R and send the completion back to SOCS (instead of manual call to MSOC/CAT.

2.2.7 DCSC Assumptions

1) DCSC will install both the NavisXtend fault and provisioning servers by
2) It is assumed that DCSC has its own trouble ticketing and management system and such functions are not provided by the NMS. Initially, no automated interface between NMS and a trouble ticketing system is provided.
3) The DCSC will be responsible for NMS Request Manual Actions (RMAs). Other systems and centers in the operations process flow [1] will be responsible for their RMAs.

2.2.8 PVC Management

1) The FastAccess service order driven PVCs will automatically be provisioned across multiple EMSs 1 day before the due date. *Since these PVCs will be provisioned automatically no manual, pre-planned provisioning will be necessary by the AWS.*

   Note: Since AWS provides the pre-planned provisioning capabilities, it is possible to manually pre-provision the DSLAMs by AWS (even before a DSLAM is installed). If such pre-provisioning is used, the entire DSLAM must be pre-provisioned for the consumer-class FastAccess service and NMS will "verify" the pre-provisioned cross-connection connection and associated profiles. For the business class, the pre-provisioned consumer class cross-connection and profiles will be changed to the ones for the business services. Upon disconnection of a business class service, all business class parameters must then be converted to the original consumer class parameters. Due to difficulty of processes associated with this approach, it is not recommended.

2) For DSLAM PVC provisioning, the associated service profiles (e.g., ATM, ADSL) will be specified as a part of ADSL port provisioning command. The traffic descriptor profile will be specified as a part of DSLAM cross-connection command. The service profiles are defined consistent with service definition and are stored in DSLAMs.
3) For the ATM PVC provisioning, since Ascend Provisioning Server does not support the concept of profiles, ATM and traffic descriptor profiles must be provided in NMS.
4) There is a "unique" machine selected PVC ID associated with each PVC (i.e., VCC or VPC) (See Figure 2-4). Specific convention for the format of the PVC ID is proposed in this document.

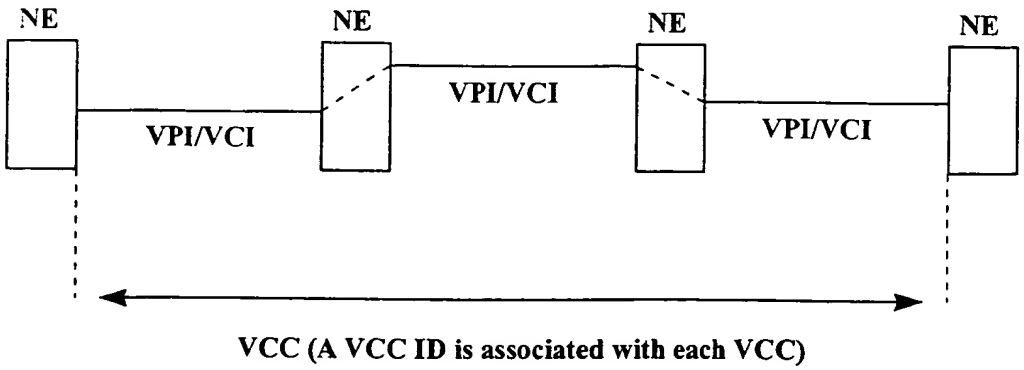

Figure 2-4. Demonstration of VCC (End-To-End Entity) and Associated VCC ID

2.2.9 NMS vs. EMS Functions

1) The EMSs will be involved in the installation of a DSLAM, SG, ATM switches, and physical facilities (DS1/DS3/OC3/OC12). Upon such installation, the FastAccess related equipment, facilities, and locations object instances will then be created in NMS database for subsequent NMS initiated logical provisioning. When a new DSLAM is created in the NMS database, an event will automatically be generated that invokes a dialog with that DSLAM to retrieve its inventory.
2) Only a frequently used subset of TL1 commands will be supported in NMS. To access all TL1 commands, the NMS user may "cut-through" to AWS GUI. An example of a less frequently used TL1 command is SET SID/TID, which is only used at installation time.
3) The NMS and AWS databases should be synchronized as much as possible. Since the AWS TL1 command line interface does not support "auto-discovery" messages for network configuration in Release 1, it will be attempted to synchronize the NMS and AWS databases by retrieving (i.e., refreshing) the logical and physical inventories. In Release 2 and beyond, this database synchronization will be based on the auto-discovery messages received from the AWS.
4) Any NMS function requiring "true and real-time" data, should retrieve such data from source of the data, i.e., DSLAMs.
5) The NMS is responsible for managing end-to-end logical entities across EMSs. Examples of these logical entities are VCC and VPC. The NMS functions will be complementary to the EMSs and will not duplicate the AWS and NavisCore functions. However, some duplication of EMS data may be necessary for NMS to perform its "end-to-end" and cross-EMS management functions.

2.2.10 DSLAM Inventory and Port Selection

Although the DSLAM may be fully loaded with splitters, it will not be fully loaded with ATU-C cards for the mass service offering. In Release 1, the inventory of CO- DSLAM will be known to COSMOS and the inventory of R-DSLAM will be known to LFACS. The COSMOS/LFACS will then select the next available port from their respective inventories and include that as part of the SOCS pending service orders that are forwarded to NMS.

Note: In the subsequent releases, the port selection function will be considered to be performed by NMS. Only NMS knows the "real time" status of DSLAM inventory including state of the ADSL ports. That is, the DSLAM ADSL ports may be out-of-service, "operationally" or "administratively." Such information will not be known to COSMOS/LFACS and COSMOS/LFACS may select such ports causing a RMA in the NMS.

2.2.11 Fault Management Assumptions

1) The NMS will receive all FastAccess related alarms/events. NMS will send a copy of TL1 alarms that are related to DS1/DS3/OC3 facilities terminating on DSLAMs to NMA for NMA alarm correlation (NMA will accept "out of sequence" alarms and does not monitor ATAGs). The delivery of alarms to NMA is subject to Alcatel and Bellcore performing the appropriate OSMINE functions for AWS TL1 interface.
2) The NMS will not forward to NMA any of the SNMP traps that are received from the NavisXtend fault server. It is assumed that the DCSC will send those alarms to NMA through an alternative arrangement.
3) Initially, the NMS will only monitor the Ascend ATM edge switch ports that are used by the FastAccess service. This includes the physical port traps, logical port traps, and VP/VC traps (e.g. "Circuit Down/circuit rerouted" traps that indicate the connection across the ATM subnetwork that is down/rerouted). The links in the middle of the ATM network will not be monitored by the NMS (NavisCore or NavisXtend Fault Server will monitor those). It is also assumed that any hard failure in the middle of the network will be propagated to the impacted edge switch by use of SONET and ATM layer (i.e., VP/VC layer) alarms such as AIS and RDI.
4) The third-party installer who installs ATU-R will test the end-to-end service by connecting to ISPs/Corporate LANs to insure connectivity. Hence, no pre-service testing from NMS will be supported in Release 1 of NMS.

2-14

3. NMS Generic Requirements

This section provides generic requirements, some of which are covered more specifically in subsequent sections.

3.1 "Cut-Through" Capability

3.1.1 Purpose

The NMS will interface with multiple EMSs and, potentially, directly with some network elements. The *"cut-through" capability* refers to the ability to perform operations directly in an Element Management System (or network element, as appropriate) from an NMS operator console.

In Release 1, the cut-through capability gives an operator at an NMS operator console the ability to directly access the AWS, NavisCore, and DANA/SMC GUIs via X-windows sessions. This feature is used to:

- ⇒ Provide the EMS capabilities to the NMS user from the single NMS terminal
- ⇒ Enable the NMS user to perform physical/equipment level installation and provisioning using the EMS functions
- ⇒ Allow advanced troubleshooting, where equipment/configuration details normally too "low level" for the NMS are needed to resolve network or service troubles.

3.1.2 Dependencies

None.

3.1.3 Feature Description and Flow

This feature is initiated by the operator (user) via either point-and-click or typed command. This initiates an EMS session and gives the user access to the EMS login screen.

3.1.4 Requirements

G-NMS-1 The FastAccess NMS *shall* allow remote operator access to the AWS, NavisCore, and DANA/SMC. This will include the ability to have complete remote control of the EMS GUI interface from a window (or windows) on the NMS operator station.

G-NMS-2 When multiple instances of an EMS exist (e.g., multiple AWS) the NMS *shall* have the ability to cut-through to the proper instance of an EMS given, based on object-specific information (e.g., a specific EMS, DLSAM, or customer ID).

G-NMS-3 X-windows is a UNIX-based function, which is outside of (and complementary to) the main NMS functionality being constructed on OSI's NetExpert™ framework. That is, this level of "remoting" the EMS GUI is independent of NetExpert, and can be controlled from the UNIX command line. However, it is required to seamlessly integrate the cut-through functionality with the remainder of the NMS 'look and feel,' including launching remote GUI sessions from menus within the NMS system and via single mouse clicks from a limited set of graphics objects.

Explanation/Example: Implementing menu-driven access to the EMS GUIs can be accomplished via menu commands constructed in the *.netexpertrc* configuration file, as in the following example:

```
menu.default:
Label: Open CascadeView GUI
Command: $OSI_HOME/openCascadeViewXterm
```

where the executable file $OSI_HOME/openCascadeViewXterm contains the appropriate shell script, e.g.,[1]

rsh <system>:<CascadeView GUI startup> -DISPLAY $DISPLAY

Likewise, the NMS GUI may have relatively high-level graphical views of switches, DSLAMs, or subnetworks. The ability to 'click-through' from high-level views supported via the NMS GUI to detailed equipment views supported via the EMS GUIs can be supported in a similar fashion via constructing similar menu entries in the *.netexpertrc* file associated with specific graphical objects, e.g.

```
menu.DSLAM:
Label: Open AWS GUI
Command: $OSI_HOME/openAWSXterm $managedElementId
P: Verify: DSLAM Identifier: #managedElementId;
$managedElementId
```

where the $OSI_HOME/openAWSXterm script can contain additional input to instruct the AWS GUI to open the appropriate view.

[1] In practice, it will be better form to first check to see if such a process is already running, and if so maximize that window instead of duplicating the process.

3.2 Selective NMS Grouping and Ranging Across DSLAMs (R1)

3.2.1 Purpose

The purpose of this requirement is to help the NMS user avoid issuing repeated TL1 commands for the same function (e.g., retrieving inventory) across multiple DSLAMs.

3.2.2 Dependencies

None.

3.2.3 Requirements

G-NMS-4 To perform the same operations across DSLAMs, the NMS user shall be able to specify a subset or all of the subtending DSLAMs by specifying the DSLAM TIDs or a file consisting of those TIDs.

Note: The specific operations for which the capability must be supported are subsequently specified. This requirement implies that NMS must have the knowledge of all its subtending DSLAMs TIDs that are part of the inventory feature.

3.3 Assignment of a PVC ID to Each PVC (R1)

3.3.1 Purpose

TIRKS will assign a Circuit ID (CID) associated with the physical facilities (e.g., OC3 and DS3). The CID is a way to identify the facilities for internal operations purposes as well as cross-administration communications.

The intent of this requirement is to extend the same concept of a physical CID to end-to-end ATM logical circuits such as VCC (Virtual Circuit Connection) or a VPC (Virtual Path Connection) (see Figure 2-4). For the FastAccess service, the following VCCs and VPC are identified that *require* associated PVC IDs:

- ⇒ A VCC between ATU-R and Service Gateway
- ⇒ A VCC between Service Gateway and NSP
- ⇒ A VPC between DSLAM and Service Gateway
- ⇒ A VCC between ATU-R and NSP (i.e., a direct connect, without going through the Service Gateway).

3.3.2 Requirements

G-NMS-8 NMS shall automatically assign a *"unique"* machine selected PVC ID to any VCC or VPC that is created by NMS. The unique PVC ID shall be stored in NMS until the PVC is disconnected. At that time, the PVC ID shall be automatically removed.

G-NMS-9 The following conventions shall be used as the PVC ID for the above four PVC types:

- ⇒ For a VCC between ATU-R and Service Gateway, the following convention for PVC ID shall be used: "TN + VPI/VCI of the ADSL access link."
- ⇒ For a VCC between Service Gateway (i.e., DANA) and NSP, the following convention for PVC ID shall be: "DANA CLLI[2] + NSP Physical Circuit ID."
- ⇒ For a VPC between DSLAM and Service Gateway (i.e., DANA), the following convention for PVC ID shall be: "DSLAM CLLI + DANA CLLI VPI at DSLAM."
- ⇒ For a VCC between ATU-R and NSP (i.e., a direct connect without going through the Service Gateway), the following convention for PVC ID shall be used: "TN + VPI/VCI of the ADSL access link."

G-NMS-10 When NMS provisions an ATM circuit through the NavisXtend Provisioning Server, it shall assign the same PVC ID across the Ascend cloud as the one selected by the NMS. Hence, the same PVC ID shall be used in NMS as well as NavisCore/NavisXtend.

3.4 DANA to NSP Connectivity (R1)

3.4.1 Requirements

G-NMS-11 The NMS user shall have the capability to query the NMS database to determine the list of NSPs that are logically connected to the specified Service Gateway. The NMS user shall also be able to retrieve the corresponding PVC IDs for PVCs between DANA and NSP.

3.5 Use of AWS TL1 Messages by NMS (R1)

3.5.1 Requirements

G-NMS-12 Although use of CTAG is stated to be optional [2], it shall always be used for all TL1 commands initiated from the NMS.

G-NMS-13 If a TL1 message is issued by NMS and there is no response corresponding to that message, NMS shall issue a second command, but it shall have a different CTAG.

G-NMS-14 At the time of the installation of a DSLAM, the SID/TID of the DSLAM shall be provisioned as CLLI of that DSLAM.

[2] COMMON LANGUAGE is a registered trademark, and CLEI, CLLI, CLFI, and CLCI are trademarks of Bellcore.

Since AWS communicates to DSLAM via SNMP, it does not name the DSLAMs based on TID and it has a different naming convention. To unify the NMS and AWS naming convention, it is recommended that AWS user selected name for a DSLAM be the same as the CLLI code of that DSLAM.

3.6 Handling of Service Orders By the NMS (R1)

3.6.1 Requirements

G-NMS-15 The NMS user interface shall support entry of new, certain change orders, and disconnect service orders. The change orders subsequent to the service order completion will be RMAed and handled manually.

G-NMS-16 NMS shall be able to automatically process and provision (in a flow-through manner) new and disconnect service orders that are received via the SOCS/NMS interface.

G-NMS-17 (O) The NMS user shall be able to automatically pull-up, edit, and re-submit for processing any of the service orders that are RMAed by NMS. The NMS user shall be able to pull-up such service orders by specifying the customer ID (i.e., TN). Upon inputting the TN, the user shall be provided with a list of service orders numbers associated with that customer. Clicking on a specific service order number, the RMAed service order shall be pulled up for editing and re-submitting.

G-NMS-18 The NMS shall provide a mapping of COSMOS and LFACS naming conventions for DSLAM and R-DSLAM ports to Alcatel naming convention for the same ports.

3.7 Identification of Network Resources Associated With a Customer (R1)

3.7.1 Purpose

The purpose of this feature is to identify the associated network resources for a given customer ID (i.e., TN).

3.7.2 Requirements

G-NMS-19 Given a Customer ID (i.e., TN), NMS shall specify a list of the PVC IDs associated with that TN. Clicking on a specific PVC ID, NMS shall provide an end-to-end pictorial representation of that specified PVC with all associated specifications. NMS shall specify the sequence of VPI/VCIs and associated ports which make up that PVC. Furthermore, the associated physical facilities (e.g., OC3, DS3) which the PVC traverses shall also be specified together with their Circuit Ids.

G-NMS-20 (O) Clicking on a physical Circuit ID in a GUI pictorial representation, NMS shall provide a list of all PVC IDs associated with that physical circuit. This is an on-demand *physical to logical mapping* and may be used for diagnostic purpose. or example, if the pictorial representation of the PVC indicates a "red" physical facility (i.e., it is alarmed), then clicking on the facility CID, the NMS will provide all the impacted PVCs and associated customers.

3.8 Availability of Customer Data To NMS User (R1)

3.8.1 Purpose

The purpose of this feature is to make available to the NMS user the customer information. The information includes the Customer Name, Customer address, Customer contact number, Type of service, Customer ID, Service Order number, Serving COs, Serving DSLAM, customer port ID, PVC IDs associated with each port, and NSPs associated with each customer. This type of information shall be stored only for the FastAccess customers.

3.8.2 Dependencies

An interface to SOCS for obtaining the "pending" Service Orders (SOs) is needed. The pending orders should provide the required customer data. If the number of customers become so large that storing such data could have adverse impact on the NMS performance, such data should be kept in a separate database/system (could be an external database accessible by both NMS and future SMS users).

3.8.3 Flow

1) The NMS obtains the pending business service orders from the SOCS.
2) The NMS parses the SO and obtains the available customer information. At this point, all information associated with that customer should be obtainable from the SO.
3) The NMS stores the customer data in NMS or another system or database that is easily accessible by the NMS user.

3.8.4 Requirements

G-NMS-21 NMS shall be able to parse the SOCS service orders and obtain the required customer records. NMS shall store key customer information such as Customer ID.

G-NMS-22 (R2) NMS shall store the customer data for future access by the NMS user. The information includes the customer name, customer ID (i.e., TN), customer address (business customers only), customer contact number (business customers only), type of

service, serving CO, serving DSLAM, customer ATU-C port, PVC IDs associated with each DSLAM port, and NSPs associated with that customer.

G-NMS-23 (R2) Specifying a Customer ID (i.e. TN), DSLAM Port ID, or ATM PVC ID, the NMS user shall be able to retrieve the customer record.

3-8

4. Network Creation Requirements

4.1 Purpose

NMS Network Creation features are intended to be used by FastAccess network and service support staff and the FastAccess NMS system administrator. The purpose of the Network Creation features is to maintain an accurate view of the physical and logical network inventory related to FastAccess services. These features include the following:

- Provide NMS user interfaces for managing the creation and inventory of the physical network equipment supporting FastAccess services. This equipment includes Alcatel's DSLAMs and Service Gateways. In addition, the physical links between this equipment and customer NSPs and the physical ports on an ATM switch (currently consisting of Ascend's ATM switches) that make up the ATM subnetwork will be inventoried.
- Representation of the network topology, which includes the network equipment and physical and logical ATM connections between a DSLAM and an ATM switch, between the ATM switch and the Service Gateway (DANA), between an ATM switch and the NSP, and the logical connections between ATM switches on the subnetwork that support the ADSL FastAccess services.
- Icon representation of the Element Management Systems (EMSs) that are used to manage the equipment, which includes the Alcatel AWSs to manage DSLAMs and Ascend's NavisXtend to manage the ATM subnetwork will be available on the NMS workstations.
- An NMS user interface (and scheduled process) to discover the configuration of a DSLAM, providing the capability to monitor the inventory of DSLAMs.

4.2 Dependencies

Network creation is used to establish the physical and logical network database and assignable resources and services that will be used to support all FastAccess services in NMS.

The Network Creation process relies on the WORD document from TIRKS to provide the physical links and physical port assignments that make up the connectivity of the ADSL network, as well as the Engineering Work Order from LFACS and COSMOS to support the service order assignments.

The support of PVC management, Fault Management (FM) and in subsequent releases, testing and Performance Management (PM) functions depend on the creation of this network database. All FastAccess end-customer general information and service configuration (i.e., assigned network resources and logical ATM connections) will flow from the service orders and is addressed in the PVC management section.

4.3 Assumptions

The assumptions used in the development of Network Creation requirements are as follows:

- The ATM physical link between the ATM subnetwork and each NSP may be used for other ATM services and is not restricted to FastAccess service.
- All ATM switch ports on the ATM subnetwork may be used for other ATM services and is not restricted to FastAccess service.
- States and their related LATAs will reside in the NMS database at initialization.
- A real ATM subnetwork already exists, managed by a NavisCore EMS.
- An ATM subnetwork object already exists in the NMS database when it is first brought up.

4.4 Terminology in this Section

The term ATM physicalPort denotes any one of the following object classes:

- AtmDs1Port
- AtmDs3Port
- AtmOc3Port
- AtmOc12Port.

The term ATM physical link denotes a carrier circuit carrying ATM PVCs and may be any one of the following object classes:

- DS1
- DS3
- OC3
- OC12.

The term Building Location is used to denote either a Central Office location or a remote location (e.g., controlled environmental vault). This location is defined by the 8-character CLLI code. An additional 3-character entity code to further describe the equipment may be used, resulting in an 11-character CLLI code.

In place of the telephone operating company term RMA (Request for Manual Assistance) the more generic term user alert is used.

4.5 Model of Network Represented in NMS

The FastAccess database objects are specified in the Object Model Design Document [7]. The following is a description of the model of the ADSL network that will be supported in the NMS database.

4.5.1 NMS Database Object Representation

The components of the network that will be represented in the NMS database as objects are as follows:

- Alcatel DSLAM
- serviceGateway - Alcatel Service Gateway (DANA)
- ATM Switch - CBX500 (Cascade)
- dslamCard - A plug-in tracked in FastAccess on the dslam. A type attribute allows dslamCards of the following types:
  - type LT [2] - This is the ATU-C plug-in. A dslamCard, type LT, supports four ATU lines or circuits.
  - type NT - This is the card supporting the OC3, OC12 or DS3 ATM link to the ATM subnetwork. A dslamCard, type NT, supports an ATM physicalPort that terminates an ATM link.

A plug-in on the dslam that is not tracked in the NMS database is the Low-Pass Filter (LPF) card, described in [2]. For each dslamCard, type LT, there has to be provisioned an LPF card in the slot directly above it. The LPF card is referred to as a POTS Splitter in the PC/DNA Market Trial Methods and Procedures document [8].

- location - Locations may be of types: Building Location or NSP Point Of Presence (POP).
- Subnetwork-ATM subnetwork.
- physicalPort, sub-classes-AtmDs1Port, AtmDs3Port, AtmOc3Port, AtmOc12Port, ADSLPort. Servicegateway ports will use the ATMOc3Port.
- terminationPoint, sub-classes: vpTP, vcTP.
- crossConnection - Cross-connect across DSLAM.
- SubnetConnection - Connection across ATM sub-network.
- pvc - ATM PVC across ADSL network. Sub-classes: vpcPVC (Virtual Path Connection), vccPVC (Virtual Channel Connection).
- PhysicalLink - Any kind of circuit transferring data. The link sub-classes that are of interest in this section are those that are carrier circuits for the ATM PVCs. These are: DS1, DS3, OC3, and OC12.
- customer - Object representing a single customer. The key attribute of customer is primary telephone number. Customers may be of types: ADSL customer or NSP customer. An NSP customer is a corporation that owns NSP with one or more NSP POP locations in the FastAccess network.
- fastAccessService - An instance of service ordered by a FastAccess customer. The key attribute of fastAccessService is the telephone number of the ADSL metallic loop. A single customer may be associated with one or more FastAccess Services.

Figure 4-1 shows a model of the primary components that make up the FastAccess network in NMS.

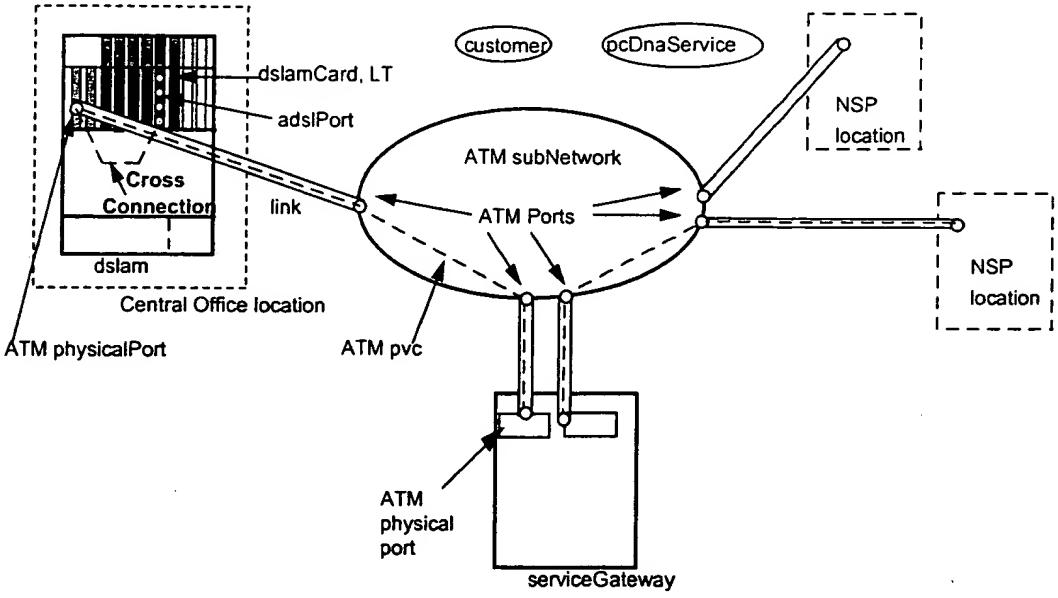

Figure 4-1. Model of FastAccess Network in NMS

4.5.2 ATM Subnetwork

There is one ATM subnetwork3 in the NMS database.

4.5.3 Locations

There are multiple Building Locations and NSP locations. On a top-level view of the entire FastAccess network on the GUI, the States are in geographically appropriate positions.

A location type of NSP is modeled as a black box. There may be one or more ATM physicalPorts on an ATM switch associated with an NSP location.

A location type of Building Location is modeled as a white box, containing managed elements such as a DSLAM, an ATM switch, or a serviceGateway. One or more DSLAMS, ATM switches, or serviceGateways may be located at a Building Location. A DSLAM located in a remote location is treated the same as a Building Location (Central Office) DSLAM. It will have its own unique CLLI code to identify the building or residence (e.g., a Controlled Environmental Vault [CEV]) of the physical equipment.

[3] By assumption in Phase 1.

4.5.4 Network Elements

The Network Element classes modeled are: the DSLAM, ATM Switch, NSP, and the serviceGateway. Network Elements are located at Building Locations.
A DSLAM is connected to the ATM subnetwork by a single ATM link. The DSLAM is modeled internally as described in Section 4.5.6.

An ATM Switch is connected to the ATM subnetwork that supports FastAccess services. A serviceGateway is connected to the ATM subnetwork by one or more physical links. A serviceGateway is modeled as having slots 1-6, Port 0. Each slot supports an ATM physicalPort that may terminate an ATM physical link. (For this release, it is assumed that all slots terminate ATM).

An NSP is a location that has one or more physical links to the ATM switch and does not have any physical inventory tracked by the NMS.

4.5.5 Physical Links and ATM Physical Ports

A physical link is any kind of circuit transferring data. The physical link sub-classes that are frequently referred to in this section are those that are carrier circuits for ATM PVCs. These are DS1, DS3, OC3, and OC12.

The following physical links are tracked in FastAccess:

- DSLAM<-->ATM Subnetwork
- ServiceGateway<-->ATM Subnetwork
- NSP location<-->ATM Subnetwork.

An attribute of a physical link is the CLFI code. This is the Circuit ID that is identified in TIRKS when the carrier circuit is first created, prior to installation in the physical network. A CLCI code format supports the physical link(s) ordered by the NSP customer.

Each physical link is terminated at either end by an ATM physical port. ATM physicalPort object types are: AtmDs1Port, AtmDs3Port, AtmOc3Port, or AtmOc12Port.

An ATM physicalPort object may be on:

- a DSLAM NT card, or a serviceGateway slot/port
- a location type of NSP
- an ATM switch in the ATM subnetwork.

4.5.6 DSLAM Model

A DSLAM contains up to four racks [2]. A rack contains up to four shelves. Each shelf contains 12 slots for Low-Pass Filter (LPF) cards (not inventoried in NMS database) and

12 slots for dslamCards of type LT (Figure 4-2). A shelf also has two slots that may have dslamCards of type NT.

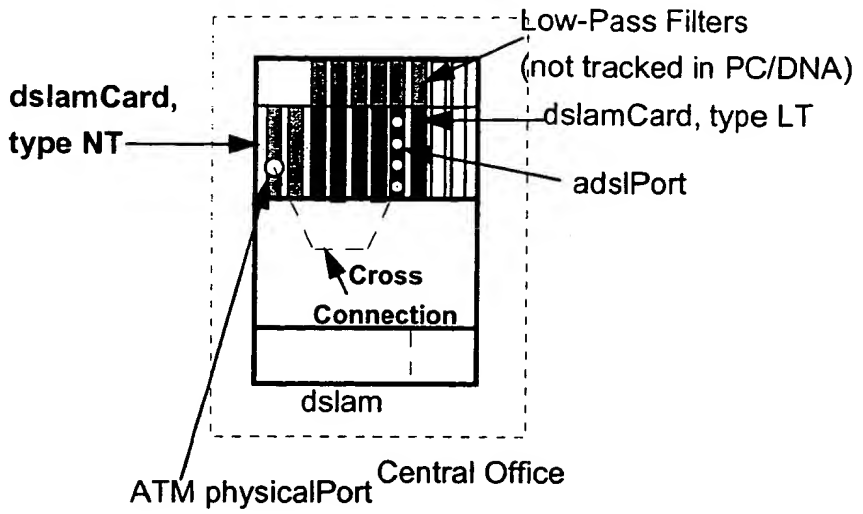

Figure 4-2. DSLAM Model

A dslamCard type LT supports four ATU-C terminations, that is, it has 4 adslPorts.

Each DSLAM has two NT type dslamCards in its top-most shelf. The primary dslamCard type NT (the secondary is a stand-by) supports an ATM physicalPort at one end of a physical link connecting the DSLAM to the ATM subnetwork.

4.5.7 Remote DSLAMs

A remote DSLAM may be located in a non-Central Office building location. However, the physical location of the remote DSLAM has a CLLI code that will describe its residence. Therefore, remote DSLAMs will not be treated differently than a DSLAM that resides in a Central Office building. Figure 4-3 is an example of a remote DSLAM that interconnects with the ATM subnetwork via an ATM switch in a Central Office building location.

4-6

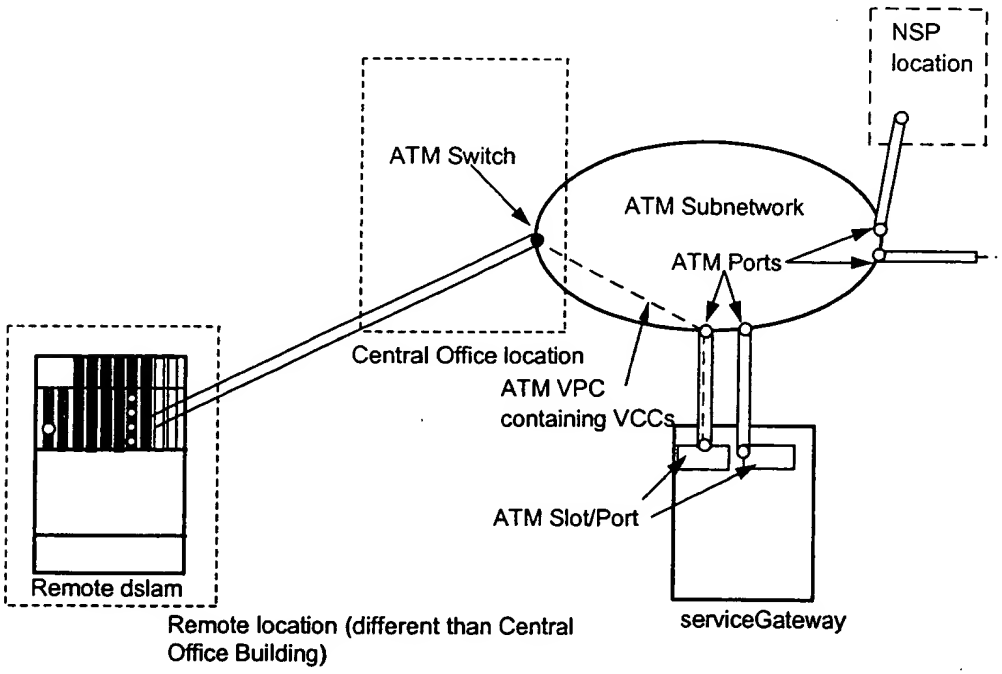

Figure 4-3. Remote DSLAM

There is an ATM physical link from the Remote DSLAM to the Central Office building location ATM switch. At the Remote DSLAM, the link is terminated by a physicalPort on a dslamCard type NT. At the Central Office, the physical link is terminated on a physicalPort of an ATM switch.

All the Virtual Channel Connections (VCCs)from the Remote DSLAM are grouped into a single Virtual Path Connection (VPC). This VPC rides the physical link to the ATM subnetwork.

4.5.8 ATM PVCs

A subNetConnection is a portion of an ATM PVC across the ATM subnetwork. A subNetConnection is between two ATM physicalPorts on the edges of the ATM subnetwork.

A PVC is an ATM PVC across the entire ADSL network (which includes the ATM subnetwork). ATM PVCs are sub-classed as vpcPvc and vccPvc.

ATM PVCs may be between an:

- (adslPort on a DSLAM)<--->)(ATM physicalPort on serviceGatewayCard on a serviceGateway)
- (ATM physicalPort on serviceGatewayCard)<--->(ATM physicalPort on a NSP location)
- (adslPort on a dslamCard)<--->(ATM physicalPort on a NSP location).

A portion of each of these ATM PVCs will traverse the ATM subnetwork.

An ATM physicalPort may have 0 or more PVCs terminating at it. Each termination of an ATM PVC at a port is marked by a terminationPoint. If the terminationPoint terminates a VCC, it is called a vcTP. If it terminates a VPC, it is called a vpTP.

4.5.9 Grouping VCCs into VPCs

There are two cases where VPCs are used.

- Virtual Channel Connections go across the ATM subnetwork (Figure 4-3).
- A serviceGateway may support multiple DSLAMs. All the VCCs from a particular DSLAM to a serviceGateway are grouped into a single Virtual Path Connection, a vpcPvc, between an (ATM physicalPort for a DSLAM)<-->(ATM physicalPort for a serviceGateway). This way it is possible at the serviceGateway to distinguish which VCCs are from which DSLAM.

4.6 High-Level Process Flows

The following flows describe at a high-level the user actions in the physical network and resulting actions in the NMS with respect to Network Creation.

4.6.1 Network Creation for the Embedded Base

When the NMS is first brought up, there will be an existent FastAccess network with installed equipment. The NMS will also contain the Network Map for all the States in the BellSouth Region. The relationship of the States to the LATAs represented by a major city in each LATA will also exist. To bring the NMS up-to-date with the existing network, the following overall flow should be used.

- For each Building Location (e.g., Central Office) that is part of the FastAccess network, the user creates a Building location object in the NMS database.
- For each physically existing DSLAM in the NMS database, the user creates a dslam object in its Building location. The creation of the dslam object causes the NMS to get the configuration of the existent DSLAM and populate itself with the racks, shelves, and slots that are associated with the card configurations of the existent DSLAM.
- The user creates appropriate ATM Switch objects (as needed).
- The user creates appropriate ATM physical ports on the edge of the ATM subnetwork.

- For each physically existing Service Gateway in the NMS database, the user creates a serviceGateway object in its Building location.
- For each existing NSP in the NMS database, the user creates an NSP location.
- The user creates appropriate physical links between the DSLAM and the ATM subnetwork, the NSP and ATM subnetwork, and the Service Gateway and the ATM subnetwork.

4.6.2 Allowable Order of Creation and Deletion of Inter-Dependent Objects

Table 4-1 indicates the order in which the user may create inter-dependent objects in the NMS.

Table 4-1. Order of Creation of Inter-Dependent Objects

ATM Subnetwork (Pre-exists)		
location (type Building Location, NSP)		
dslam	serviceGateway	NSP
dslam racks, shelves (automatically created by dslam_GetConfiguration)		
dslamCard (automatically created by dslam_GetConfiguration)	serviceGateway Slot/Port (automatically created by NMS upon Gateway creation)	
physicalPort: AdslPort, AtmDs1Port, AtmDs3Port, AtmOc3Port, or AtmOc12Port		
Physical link: DS1, DS3, OC3, or OC12		
ATM pvc: vpcPvc or vccPvc	customer	fastAccessService

Table 4-2 shows the order in which the user may delete inter-dependent objects in the NMS.

Table 4-2. Order of Deletion of Inter-Dependent Objects

ATM pvc: vpcPvc or vccPvc		customer		fastAccessService		
Physical link: DS1, DS3, OC3, or OC12						
physicalPort				DSLAM	NSP	Service Gateway
location (type Building Location, NSP)						
ATM subNetwork (never deleted)						

In this release, the user does not have the capability to delete individual components of a Network Element in the NMS database. The deletion of a dslam object causes the automatic deletion of all racks, shelves, associated cards, and physical ports associated with the dslam object. The deletion of a serviceGateway object causes the automatic deletion of all slots, ports, and port types associated with the serviceGateway.

4.7 Feature Description: Feature Flows within the NMS

This section describes the high-level steps to be taken for the creation and deletion of each network component and the physical links between these components that make up the FastAccess network in NMS User Alert messages that relate to the creation and deletion of these network components are described in Section 12.

4.7.1 Creation of a New Location Object in the NMS Database

Prerequisites
None.

Flow

- On the appropriate NMS GUI screen, the user creates new location objects.
- The user enters generic location parameters. These are:
  - Type of location: Building Location or NSP
  - CLLI code for building location (English name for the NSP)
    - ⇒ City code (4 characters)
    - ⇒ State (2 characters)
    - ⇒ Network site (2 characters) this completes the building location,
    - ⇒ Network entity code (3 characters, further defines equipment),
  - Street address (for all location types)
  - LATA. (for all location types)

- The new location object is created and committed to the database.
- If the location is of type NSP POP, then the user additionally associates the location with a customer object, of type NSP. Thus, for NSPs, there is a single NSP customer that may own multiple NSP POP locations.

4.7.2 Deletion of a Location Object

Prerequisites
Location object must exist in the NMS database.

Flow
- On the appropriate NMS GUI screen, the user deletes the location object.
- The location object cannot be deleted if:
  - the location has any DSLAM, NSPs or Service Gateways, associated with the location.
  - it has any physical ports associated with it that are associated with physical links.
- Deletion of a location object results in the deletion of the ATM physical port on the ATM subnetwork that is associated with the location object. These ports have no physical links associated with them.)

4.7.3 Creation of a New DSLAM Object in the NMS Database

The user creates a dslam object in its Central Office location in the NMS database. The user associates the dslam object with managing AWS EMS object (previously created). The creation of the dslam object causes the NMS to automatically retrieve the configuration of the newly installed DSLAM and populate the NMS with the racks, shelves, and slots associated with the card configurations and logical connections of the existent DSLAM.

Prerequisites:
- The new DSLAM is physically installed in its Building Location.
- The DSLAM is inventoried in TIRKS as a SONET edge-device. The DS3, OC3, or OC12 circuit supporting the ATM physical link between the DSLAM and the ATM subnetwork is designed in TIRKS and the circuit is physically installed.
- The NavisCore EMS is used to configure the physical link terminations on the ATM sub-network.
- From its managing AWS, the physical DSLAM is initialized, timing is set, and any necessary initialization attributes are set on the newly installed DSLAM. These attributes relate to the creation of alarm conditions and resulting messages and to the creation or modification of profiles to be applied to ATU-Cs or ATM PVCs in the physical DSLAM.
- In the NMS database, a valid managing AWS is associated with the DSLAM.

- In the NMS database, a valid building location object has been created.

Flow

- On the appropriate NMS GUI screen, the user creates new dslam objects.
- The user enters the CLLI code and the related LFACS or COSMOS name for the DSLAM. If the DSLAM is located in a Central Office building, it will have a related COSMOS name. If the DSLAM is in a remote location, it will have a related LFACS name.
- The user specifies a relationship between the new dslam object and its controlling AWS EMS object.
- Upon creation of the DSLAM by the user, NMS will automatically invoke the function dslam_GetConfiguration. dslam_GetConfiguration uses the SID to address the DSLAM over the TL1 interface and populates the dslam object with:
  - The racks and shelves associated with the cards
  - The NT cards
  - The LT cards.
- As part of this process, when a dslamCard, type NT, is instantiated, an associated ATM physical port is instantiated on the dslamCard. When a dslamCard, type LT is instantiated, four associated adslPorts are instantiated on the dslamCard.

4.7.3.1 The dslam_GetConfiguration Function

Input parameters
The DSLAM CLLI code on the appropriate GUI screen.

Algorithm
The function issues the TL1 message, RTRV-EQPT with the specifier provided as an input parameter. RTRV-EQPT will retrieve the inventory of:

- Racks and shelves associated with the cards
- dslamCards, type NT
- dslamCards, type LT.

The actions for each NT card retrieved in the physical DSLAM are as follows:

- If the dslamCard type NT object already exists in the database, no action is taken.
- If the dslamCard object does not exist, a new dslamCard type NT object is instantiated and is associated with the appropriate slot. Also, an ATM physicalPort object is instantiated as appropriate and associated with the dslamCard.

The actions for each LT card retrieved in the physical DSLAM are as follows:

- If the dslamCard type LT object already exists in the NMS database, no action is taken.
- If the dslamCard object does not exist, a new dslamCard type LT object is created and is associated with the appropriate slot.
- Four adslPort objects are instantiated and associated with the dslamCard type LT.
- If within the range of LT cards retrieved, there is a dslamCard type LT in the database but no corresponding LT card was retrieved from the physical DSLAM, no notification is sent to the user by NMS. No automatic deletion in NMS will occur.

Recompute the capacity parameters, numberOfSpareADSLPorts and percentAssignedDslamCapacity.

- Using the freshly updated dslam object, the numberOfSpareADSLPorts is calculated as:
  (Total number of adslPorts in dslam) - (Total number of assigned adslPorts)
- If numberOfSpareADSLPorts < thresholdSpareADSLPorts, a user alert is logged.
- Also, the percentAssignedDslamCapacity is calculated as
  (Total number of assigned adslPorts) X 100 (Total DSLAM adslPort capacity)
- If percentAssignedDslamCapacity > thresholdDslamCapacityUtilization, a user alert is logged.

4.7.4 Deletion of a DSLAM Object

Deletion of a DSLAM object may be needed-to correct an erroneous entry in the database or as part of the flow to physically remove a DSLAM.

Prerequisite
DSLAM object should exist.

To remove a DSLAM, it must be verified in the NMS that the DSLAM as a whole does not support any ATM PVCs. No PVCs should exist on the DSLAM. All customers assigned to that DSLAM must be disconnected and all PVCs must be removed before any further action can take place.

- The physical link connecting the DSLAM to the ATM subNetwork upon receipt of a disconnect order from the TIRKS system has been deleted.
- The physical port on the edge of the ATM subnetwork which terminated the physical link has been deleted.

Flow

- On the appropriate NMS GUI screen, the user deletes the DSLAM object
- The delete only proceeds if-there is no physical link associated with the DSLAM. Else, the delete returns with an error and does not delete the DSLAM object.

- Deletion of the DSLAM causes the deletion of all cards associated with that DLSAM.
- Deletion of the DSLAM causes the deletion of all alerts associated with that DSLAM.

4.7.5 Addition of an ATM Physical Port to the ATM Subnetwork

This flow is required prior to the creation of a physical link to connect a DSLAM, an NSP, or a serviceGateway object to the ATM subnetwork. The flow ensures that the ATM physicalPort object stores Ascend MIB addressing information required by NavisXtend [3] for future creation of ATM PVCs through the port.

Prerequisites
ATM subnetwork.

Flow
- On the appropriate NMS GUI screen, the user creates the ATM physical port.
- The creation of a physical port on the ATM subnetwork is known as a "PPort" on a "Card" in a "Slot" on a "Switch." To create an ATM PVC in the future, an "LPort" will need to be created under this "PPort" and a "Circuit" will need to be created with its end at the "LPort."
- The creation of an ATM PVC using the NavisXtend is described by example in Chapter 4 of the Provisioning Server User Manual [3].
- The NMS user navigates to the appropriate GUI screen to create a new ATM physicalPort. (this screen should look like the Cascade Switch View screen).
- The user associates the port with the ATM subnetwork.
- The physicalPort object is committed to the database.

4.7.6 Deletion of an ATM Physical Port from the ATM Subnetwork

Prerequisites
- ATM physicalPort object should exist.
- No physical link should be associated with it.

Flow
- On the appropriate NMS GUI screen, the user deletes the physical port object
- The delete function only proceeds if:
  - there is no physical link associated with the ATM physicalPort.
  - there is no ATM pvc associated with the ATM physical port.

  Else, the function returns with an error and does not delete the object.

4.7.7 Creation of a Physical Link

Prerequisites

4-14

- A physical link has been provisioned through TIRKS and installed in the physical network. The NMS user has determined the Circuit ID of the physical link.
- Two matching ATM physical ports have been created to connect the physical link. Except in the case of an NSP location, the port will be identified as a POI or POP and is not inventoried in NMS.

Flow

- On the appropriate NMS GUI screen, the user requests that a physical link be created between the two ATM physical port locations. In the case of an NSP, the ATM physical port is created at the ATM switch and the NSP is identified as a location.
- As an attribute, the user enters the CLCI code of the physical link.

The following is an example of the Facility Circuit ID for physical links between an ATM switch and a DSLAM, or between an ATM switch and a Service Gateway:

Facility Designation	Facility Type	Location A	Location Z
1001	OC3	DNWDGA25H01	DNWDGA25W01

The Facility Type field can be used to identify the Port type-in this case, an OC3.

The length of the Circuit ID field = 12 (no need to include the A/Z locations, these are entered in separate fields on the screen).

Facility Designation = 6 alpha-numeric characters
Facility type = 6 alpha-numeric characters.

The rule should be to key on the Facility Type field to derive the port type. Valid entries in this field will be: T1 (DS1), T3(DS3), OC3, OC12.

The following is an example of a Special Service Hi-Cap Circuit Id for physical links between an ATM switch and an NSP, which is requested by the NSP customer. The example shows only the portion of the Special Service circuit ID which will be used in the Circuit ID field:

HCFJ123456BS

- The first two characters define the rate:
  HC = DS1
  HF = DS3
  OB = OC3
  OD = OC12
- the 3rd character = intraLATA or interLATA
- the 4th character = network type (ex., J = ATM
- the 5th-10th = serial #

- the 11-12 = company code or BellSouth region code.

The length of the Circuit ID field = 12

- characters 1-2 will provide the rate
- The physical link is created if the physical ports for both locations match:
  - Both physical ports must be of the same type.
  - Valid combinations are:
    - ⇒ (Port on dslamCard)<-->(Port on ATM subnetwork)
    - ⇒ (Port on serviceGateway slot)<-->(Port on ATM subnetwork)
    - ⇒ (location type NSP)<-->(Port on ATM subnetwork).

4.7.8 Deletion of a Physical Link

Prerequisites
Physical link object should exist.

Flow

- On the appropriate NMS GUI screen, the user inputs the Circuit ID, CLLI code for each location and requests a delete.
- The function only proceeds if:
  - there are no ATM PVCs associated with the link object.

  Else, it returns with an error and does not delete the object.

4.7.9 Creation of a New serviceGateway object

Prerequisites

- serviceGateway should be physically installed in the Central Office building location.
- Valid building location object has been created.
- The service Gateway is inventoried in TIRKS (as a SONET edge device). The OC3 circuits supporting the physical links between the Service Gateway and the ATM subnetwork have been designed in TIRKS and the circuits are physically installed.

Flow

- On the appropriate NMS GUI screen, the user creates a serviceGateway object.
- The user enters the CLLI code. The building location is derived from the CLLI code.
- Upon creation of the service Gateway, NMS will create the following default attributes of the service Gateway in the database:
  - Slot
  - Port
  - Port Type.

The following defaults will be created: slots 1-6, Port will always be 0, and Port type will be OC3.

Example:
Slot 1, Port 0, Port Type OC3
Slot 2, Port 0, Port Type OC3

4.7.10 Addition and Deletion of Service Gateway Ports

The ability to create and delete serviceGateway ports will be supported in Release 2 requirements. In this release, the serviceGateway ports are automatically created in NMS and access to the physical serviceGateway does not exist.

4.7.11 Deletion of a Service Gateway Object

Deletion of a serviceGateway object may be needed:
- To correct an erroneous entry in the database
- As part of the flow to physically remove a Service Gateway.

Prerequisites
- serviceGateway object should exist.
- Verify in the NMS that the Service Gateway as a whole does not support any ATM PVCs.
- No customer assigned VCCs should exist from the DSLAM to the Gateway.
- All customers assigned to that Gateway must be disconnected and all PVCs must be disconnected before any further action can take place.
- All physical links connecting the serviceGateway to the ATM subnetwork, upon receipt of disconnect orders from TIRKS, must be deleted
- The physical ports on the edge of the ATM subnetwork that terminated the physical links must be deleted.

Flow
- On the appropriate NMS GUI screen, the user inputs the CLLI code of the serviceGateway object and requests a delete.
- The delete only proceeds if there is no physical link associated with the serviceGateway object.
  Else, it returns with an error and does not delete the object.
- Deletion of the serviceGateway object causes the deletion of all serviceGateway slots and associated physicalPorts.

4.7.12 Addition of a New NSP

Prerequisites
- A new NSP is added to the physical ATM subnetwork.

- The carrier circuit supporting the physical link between the NSP and the ATM subnetwork is designed in TIRKS and the circuit is physically installed.
- Building location must exist.

Flow

- On the appropriate NMS GUI screen, the user creates a new location object type of NSP in NMS and associates the appropriate LATA for the NSP.
- On the appropriate NMS GUI screen, the user creates a new ATM physical port for the ATM switch on the edge of the ATM subnetwork.
- On the appropriate NMS GUI screen, the user creates a physical link from the ATM physical port to the NSP location. Note: *the physical port at the NSP is unknown and not inventoried in NMS.*
- On the appropriate NMS GUI screen, the user creates the PVC at the NSP using the specified VPI/VCI on the Business Order.

4.7.13 Deletion of an NSP

Prerequisites

- NSP object exists in NMS.
- Verify in NMS that all PVCs have been disconnected from the NSP to the service Gateway and/or to the DSLAM before any further action can take place.
- Verify that each physical link connecting the NSP to the ATM subnetwork upon receipt of disconnect orders from the TIRKS system have been deleted in NMS.
- Verify that the physical ports on the edge of the ATM subnetwork that terminated the physical links have been deleted in NMS.

Flow

- On the appropriate NMS GUI screen, the user deletes the NSP object from NMS.

The function only proceeds if-the above prerequisites have been completed; Else, NMS will return an error and will not delete the object.

4.8 Requirements

Descriptions of completion and error messages on a User Alert screen that NMS should provide upon user input, are in Section 4-9.

4.8.1 General (R1)

NC-NMS-1 NMS shall notify the user of any errors or User Alerts that occur during the network creation process. A description of the user input and resulting error shall be supplied to the user on the User Alert screen.

NC-NMS-2 NMS shall uniquely identify network creation errors from reported faults, provisioning notifications, service order notifications, and other NMS system generated notifications on the User Alert screen.

NC-NMS-3 NMS shall prohibit the NMS user from deleting any equipment that supports active FastAccess services for customers associated with a DSLAM port or a PVC to a Corporate LAN.

NC-NMS-4 NMS shall allow the NMS user to generate a hard copy of the network topology and equipment from an NMS GUI Report screen.

4.8.2 Locations (R1)

NMS will use LATAs to represent a "top-level" view of the locations related to the FastAccess network. It will use Building Locations within a LATA to represent the physical location of FastAccess- supporting equipment.

NC-NMS-5 NMS shall support an NMS user interface to create a Building Location or an NSP location and associate it with a LATA in NMS to be displayed on the location list for a LATA. The city code (4 characters), state code (2 characters), building location (network site) code, and street address shall be entered by the user. The NMS user shall be notified if the location cannot be created and the reason (e.g., unknown LATA/state, duplicate code). Note: In addition to the 8 characters that make up the building location, an additional 3 characters, called an entity code, may be used to further identify the equipment in that location.

NC-NMS-6 NMS shall support an NMS user interface to delete a Building Location or an NSP location from the NMS database. The NMS shall prohibit this, if any FastAccess equipment or port is assigned to the location. The NMS user shall be notified if the location cannot be deleted (e.g., does not exist, equipment assigned).

4.8.3 DSLAM (R1)

A DSLAM is a piece of equipment that has racks (1-4), shelves (1-4), slots (1-12) equivalent to ATU-Cs, Line Termination Units (4 per slot) equivalent ATU-C ports, and Network Termination Units that support the OC3 interface to the ATM network. The key Alcatel equipment identifiers are

- NT = Network Termination Unit
- LT = Line Termination Unit
- rack = Rack number (1-4)
- shelf = Shelf number (1-4)
- lt_slot = LT slot number (1-12).

The Alcatel equipment identified is used in all TL/1 messages and will need to be reflected in the NMS database.

NC-NMS-7 NMS shall maintain the DSLAM configuration for the assignable resources, including unique identification for the DSLAM itself, the NT card that supports either the DS1, DS3, or OC3 port, and the ATU-Cs and their LTs.

NC-NMS-8 NMS shall support an NMS user interface to create a DSLAM in the NMS. The user shall specify the

- CLLI of the Building Location code, which may include the 3 character entity code
- The AWS for this DSLAM
- The COSMOS name for this DSLAM as a whole, if it resides in a Central Office location and the LFACS name for this DSLAM if it resides in a remote location.

NMS shall automatically retrieve the DSLAM physical and logical inventory upon successful creation. The user shall be notified if the DSLAM cannot be created (e.g., unknown building location, unknown AWS, duplicate CLLI code).

NC-NMS-9 NMS shall support an NMS user interface to delete a DSLAM in the NMS. The deletion shall only proceed if there is no physical link or PVC object associated with the DSLAM in the NMS database. The user shall be notified if the DSLAM cannot be deleted (e.g., unknown DSLAM, FastAccess resources assigned, physical link exists).

4.8.4 ATM Switch/Physical Ports on the ATM Subnetwork (R1)

NC-NMS-10 NMS shall support the ability to create an ATM switch object based on the ATM subnetwork object in the NMS database.

NC-NMS-11 NMS shall support the ability to delete an ATM switch on the ATM subnetwork object in the NMS database. The deletion will only be permitted if there are no ATM physical ports associated with the ATM switch.

NC-NMS-12 NMS shall support the ability to add an ATM physical port object on the ATM subnetwork object in the NMS database. For each physical port, NMS shall maintain the following attributes: switch Id, slotId, and pportId. These attributes may be entered by the NMS user in association with a particular ATM physical port (user screen should look similar to Cascade View screen for consistency).

NC-NMS-13 NMS shall support the ability to delete an ATM physical port on the ATM subnetwork object in the NMS database. The deletion will only be permitted if there is no physical link or PVC object associated with the physical port.

4.8.5 Service Gateway (R1)

NC-NMS-14 NMS shall support a NMS user interface to create a Service Gateway in the NMS to be displayed in the list of Building Location equipment. The user will specify the English name location of the Service Gateway. Upon creation, the NMS will create default slots (1-6), port (0), and port type (OC3) information for the Service Gateway created. The NMS user shall be notified if the Service Gateway cannot be created (e.g., unknown Building Location, duplicate Service Gateway).

NC-NMS-15 NMS shall support an NMS user interface to delete a Service Gateway in the NMS. The deletion shall only proceed if there is no physical link or PVC object associated with the Service Gateway in the NMS database. The user shall be notified if the Service Gateway cannot be deleted (e.g., unknown Service Gateway, FastAccess resources assigned). Deletion of the serviceGateway will cause all slots, ports, and port types associated with the serviceGateway to automatically be deleted in this release.

4.8.6 Physical Links (R1)

Physical links represent the connections between:

- A DSLAM and the ATM subnetwork (one per DSLAM)
- A Service Gateway and the ATM subnetwork (multiple links per Service Gateway)
- An NSP and the ATM subnetwork (multiple links per NSP).

These physical link connections will be designed and inventoried in TIRKS and will be assigned a CLCI code.

NC-NMS-16 NMS shall support an NMS user interface to create a physical link between two appropriately matched physical ports. The matching criteria are as follows: Both physical ports must be of the same type (that is, ATM DS1 port, ATM DS3 Port, ATM OC3 port, or ATM OC12 port). Valid combinations are:

- (Port on DSLAM NT Card)<-->(Port on ATM subnetwork)
- (Port on Service Gateway slot)<-->(Port on ATM subnetwork)
- (location, type NSP)<-->(Port on ATM subnetwork).

Only one physical link may be created between two physical ports. The NMS shall store as an attribute the CLCI code for this link. As an attribute, the user enters the CLCI code of the physical link.
The following is an example of the Facility Circuit ID for physical links between an ATM switch and a DSLAM, or between an ATM switch and a Service Gateway:

Facility Designation	Facility Type	Location A	Location Z
1001	OC3	DNWDGA25H01	DNWDGA25W01

The Facility Type field can be used to identify the Port type-in this case, an OC3.

The length of the Circuit ID field = 12 (no need to include the A/Z location, these are entered in separate fields on the screen).

Facility Designation = 6 alpha-numeric characters

Facility type = 6 alpha-numeric characters.

The rule should be to key on the Facility Type field to derive the port type. Valid entries in this field will be: T1 (DS1), T3(DS3), OC3, OC12.

The following is an example of a Special Service Hi-Cap Circuit Id for physical links between an ATM switch and an NSP, which is requested by the NSP customer. The example shows only the portion of the Special Service circuit ID which will be used in the Circuit ID field:

HCFJ123456BS

- The first two characters define the rate:
  HC = DS1
  HF = DS3
  OB = OC3
  OD = OC12
- the 3rd character = intraLATA or interLATA
- the 4th character = network type (ex., J = ATM
- the 5th-10th = serial #
- the 11-12 = company code.

The length of the Circuit ID field = 12

- characters 1-2 will provide the rate.

NC-NMS-17 NMS shall be able to maintain: one physical link for each DSLAM, multiple physical links for each Service Gateway, and multiple physical links for each NSP.

NC-NMS-18 NMS shall notify the NMS user of completions and failures (invalid ATM Switch, invalid ATM port, invalid DSLAM, NSP, or Service Gateway).

NC-NMS-19 NMS shall support an NMS user interface to delete a physical link in NMS. The deletion shall only proceed if there is no ATM PVC associated with the physical link in the NMS database. The user shall be notified if the physical link cannot be deleted (e.g., unknown Circuit Id, FastAccess resources assigned).

4.8.7 NSP (R1)

NC-NMS-20 NMS shall support a NMS user interface to create an NSP in NMS to be associated with a LATA. The user will specify the English name of the NSP, a contact name, and a street address location. An NSP may have multiple locations.

4-22

NC-NMS-21 NMS shall support an NMS user interface to delete a NSP location in the NMS. The deletion shall only proceed if there is no physical link or PVC object associated with the NSP in the NMS database. The user shall be notified if the NSP location cannot be deleted (e.g., unknown NSP location, FastAccess resources assigned).

4.8.8 ATM Logical Connections

ATM logical connections between the DSLAM and the Service Gateway, the NSP and the Service Gateway, and the end-customer to a NSP are addressed in Section 7.

4.8.9 Requirements (R2)

Release 2 requirements will reflect modifications as a result of the CMISE interface to the DSLAMs, the addition of MiniRAMs into the network, and more detailed information on the configuration and support of the Service Gateways.

NC-NMS-R2 NMS shall support the ability to add or delete Service Gateway slots associated with a specified service Gateway in the NMS database. Addition of a service Gateway slot shall result in the automatic creation of an associated ATM physical port on the slot. Deletion of the slot shall result in the deletion of the associated ATM physical port.

Deletion of a slot shall only be permitted if there is no physical link or PVC associated with the ATM physical port on the slot.

4.9 Network Creation

The following User Alert messages should be displayed on a NMS user screen for the creation and deletion of the physical network inventory to support the FastAccess services.

4.9.1 Create Location Name

Includes central office, remote building sites.

Successful
Alert Name **NC-Location Create Complete**

Description: Building location (Central Office or remote location site)

Affected Object: location

Failures

Alert Name **NC-Location Create Warning - LATA Omitted**

Alert Name **NC-Location Create Warning - Street Address Omitted**

Alert Name **NC-Location Create Failed - LATA Not Found**

4.9.2 Delete Location Name

Includes central office, remote building sites and NSPs.

Successful

Alert Name **NC-Location Delete Complete**

Description: Building location (Central Office or remote location site)

Affected Object: location

Failures

Alert Name **NC-Location Delete Failed - Network Element (indicate DSLAM, service Gateway or ATM switch) associated with Location**

Alert Name **NC-Location Delete Failed - Physical port associated with Location**

Alert Name **NC-Location Delete Failed - Physical link associated with Location**

4.9.3 Create NSP

Successful

Alert Name **NC-NSP Create Complete**

Description: NSP name

Affected Object: Customer

Failures

Alert Name **NC-Location Create Warning - LATA Omitted**

Alert Name **NC-Location Create Warning - NSP Location Omitted**

Alert Name **NC-Location Create Warning - NSP Contact Name Omitted**

Alert Name **NC-Location Create Failed - LATA not found**

4.9.4 Delete NSP

Alert Name **NC-NSP Delete Complete**

Description: NSP Name

Affected Object: Customer

Failures

Alert Name **NC-NSP Delete Failed - Network Element (indicate DSLAM, service Gateway or ATM switch) associated with NSP Name**

Alert Name **NC-NSP Delete Failed - ATM Physical port associated with NSP Name**

Alert Name **NC-NSP Delete Failed - Physical link associated with ATM Switch**

Alert Name **NC-NSP Delete Failed - PVC Exists to Service Gateway**

Alert Name **NC-NSP Delete Failed - PVC Exists to DSLAM**

4.9.5 Create - DSLAM

Includes central office and remote DSLAMS.

Successful

Alert Name **NC-DSLAM Create Complete**
(includes NMS successfully retrieved the DSLAM configuration from AWS and populates the DSLAM in NMS)

Description: Alcatel DSLAM Network Element

Affected Object: dslam

Failures

Alert Name **NC-DSLAM Create Warning - AWS ID Omitted**

Alert Name **NC-DSLAM Create Warning - COSMOS/LFACS Name Omitted**

Alert Name **NC-DSLAM Create Warning - No racks, shelves and associated cards found**

Alert Name **NC-DSLAM Create Failed - Building Location name not found**

Alert Name **NC-DSLAM Create Failed - AWS not found**

4.9.6 Delete - DSLAM

Includes central office and remote DSLAMS.

Successful

Alert Name **NC-DSLAM Delete Complete**

Description: Alcatel DSLAM Network Element

Affected Object: dslam

Failures

Alert Name **NC-DSLAM Delete Completed**
(includes NMS successfully deleted all Cards and alerts associated with that DSLAM)

Alert Name **NC-DSLAM Delete Failed - PVCs exist on DSLAM**

Alert Name **NC-DSLAM Delete Failed - Physical link to ATM switch exists**

4.9.7 Create - ATM Physical Port

On the ATM subnetwork.

Successful

Alert Name **NC-PPort Create Complete**

Description: ATM Physical Port on supported Network Elements

Affected Object: physicalPort, subclasses: AtmDs1Port, AtmDs3Port, AtmOc3Port, AtmOc12Port, ADSLPort

Failures

Alert Name **NC-PPort Create Warning - Slot not input**

Alert Name **NC-PPort Create Warning - Port not input**

Alert Name **NC-PPort Create Failed - Building Location Name (CLLI) not found**

Alert Name **NC-PPort Create Failed** - IP address not found

4.9.8 Delete - ATM Physical Port

On the ATM subnetwork.

Successful

Alert Name **NC-PPort Delete Complete**

Description: ATM Physical Port on supported Network Elements

Affected Object: physicalPort, subclasses: AtmDs1Port, AtmDs3Port, AtmOc3Port,AtmOc12Port, ADSLPort

Failures

Alert Name **NC-PPort Delete Failed - PVC associated with physical port**

Alert Name **NC-PPort Delete Failed - Physical link associated with physical port**

4.9.9 Create - Physical Link - Other

Successful

Alert Name **NC-Physical Link - Other Create Complete**

Description: Physical Link connecting Network Elements (Between the ATM subnetwork and DSLAM, ATM subnetwork and a Service Gateway)

Affected Object: PhysicalLink, subclasses: DS1, DS3, OC3 and OC12

Failures

Alert Name **NC-Physical Link Create Warning - A Port information not complete (missing rack/shelf/slot/port)**

Alert Name **NC-Physical Link Create Warning - Z Port information not complete (missing rack/shelf/slot/port)Failures**

Alert Name **NC-Physical Link Create Failed - Circuit ID invalid-(not a facility ID)**

Alert Name **NC-Physical Link Create Failed - Building Location Name (CLLI) not found for Location A**

Alert Name **NC-Physical Link Create Failed - Building Location Name (CLLI) not found for Location Z**

4.9.10 Delete - ATM Physical Link - Other

Between the ATM subnetwork and DSLAM, ATM subnetwork and a Service Gateway.

Successful

Alert Name **NC-Physical Link - Other Delete Complete**

Description: Physical Link connecting Network Elements (Between the ATM subnetwork and DSLAM, ATM subnetwork and a Service Gateway)

Affected Object: PhysicalLink, subclasses: DS1, DS3, OC3 and OC12

Failures

Alert Name **NC-Physical Link Delete Failed - Circuit ID not found**

Alert Name **NC-Physical Link Delete Failed - CLLI not found for Location A**

Alert Name **NC-Physical Link Delete Failed - CLLI not found for Location Z**

Alert Name **NC-Physical Link Delete Failed - PVC associated with the physical link**

4.9.11 Create - Physical Link - NSP

Between the ATM subnetwork and an NSP.

Successful

Alert Name **NC-Physical Link - NSP Create Complete**

Description: Physical Link connecting ATM subnetwork and NSP Name

Affected Object: PhysicalLink, subclasses: DS1, DS3, OC3 and OC12

Failures

Alert Name **NC-Physical Link -NSP Create Failed - ATM switch port information not complete - missing (insert: rack/shelf/slot/port)**

Alert Name **NC-Physical Link -NSP Create Failed - NSP name not found**

Alert Name **NC-Physical Link -NSP Create Failed - NSP Location not found**

Alert Name **NC-Physical Link -NSP Create Failed - Circuit ID invalid-(not a special service circuit ID)**

Alert Name **NC-Physical Link -NSP Create Failed - Building Location Name (CLLI) not found for ATM switch port**

4.9.12 Delete - ATM Physical Link - NSP

Between the ATM subnetwork and NSP.

Successful

Alert Name **NC-Physical Link - NSP Delete Complete**

Description: Physical Link connecting ATM subnetwork and NSP Name

Affected Object: PhysicalLink, subclasses: DS1, DS3, OC3 and OC12

Failures

Alert Name **NC-Physical Link -NSP Create Failed - Circuit ID not found**

Alert Name **NC-Physical Link -NSP Create Failed - CLLI not found for ATM port location**

Alert Name **NC-Physical Link -NSP Create Failed - PVC associated with the physical link**

4.9.13 Create - Service Gateway

Successful

Alert Name **NC-Service Gateway Create Complete**
(includes NMS auto populate serviceGateway object with all slots/ports and port type)

Description: A service Gateway is connected to the ATM subnetwork by one or more physical links.

Affected Object: serviceGateway

Failures

Alert Name **NC-Service Gateway Create Failed - Building Location Name not found**

Alert Name **NC-Service Gateway Create Failed - LATA not found**

4.9.14 Delete - Service Gateway

Successful

Alert Name **NC-Service Gateway Delete Complete**
(NMS will automatically delete all slots/ports and port types associated with the service Gateway)

Description: A service Gateway is connected to the ATM subnetwork by one or more physical links.

Affected Object: serviceGateway

Failures

Alert Name **NC-Service Gateway Create Failed - ATM PVC exists**

Alert Name **NC-Service Gateway Create Failed - Customer assigned VCC exists**

Alert Name **NC-Service Gateway Create Failed - Physical link exists**

5. Capacity and Inventory Management Requirements

This section discusses the DSLAM physical inventory and capacity management. The logical inventory is addressed in the PVC provisioning section.

Although capacity and inventory management are covered in this section, it must be noted that they are distinct and independent functions. Hence, there is no correlation between the two functions and the data from one function should not be used for the other. The amount of inventory data (which includes physical and logical inventory) is significantly more than capacity management data. Furthermore, for the inventory data, NMS database will be refreshed less frequently (e.g., per week). The inventory refresh consists of the entire physical and logical DSLAM inventory and may be performed on-demand or periodically. On the other hand, the capacity management data will be restricted to DSLAM port status and should be retrieved more frequently (e.g., every few hours).

Since the ADSL loop is not TIRKS designed and inventoried, the inventory systems normally used for special services flow are not used [1]. Hence, the intent of this section is to provide the capacity and inventory management capabilities in the NMS to support appropriate capacity planning and inventory centers.

5.1 DSLAM Capacity Management and Thresholding

5.1.1 Purpose

The purpose of this feature is to provide:

- Information on number of "equipped and available for assignment" DSLAM ATU-C ports and provide an alert when the number of such ports goes below a user-settable threshold
- An indication of when the DSLAM capacity is near exhaustion so that another DSLAM can be ordered
- An indication of how fast the ADSL ports have been put into service within the past "n" days (the number "n" may be user-settable)
- An automated way of providing the DSLAM capacity information to appropriate capacity planner or capacity planning center.

The ADSL ports in the DSLAM provide information on a port's "operational" and "administrative" states. A DSLAM port may be operationally "in-service" or "out-of-service." It may also be administratively "in-service" or "out-of-service." A DSLAM port that is operationally or administratively "out-of-service" should be used to create a PVC on that port. Hence, NMS must check the operational and administrative states of the DSLAM ports before a cross-connect is made.

From the DSLAM perspective, the "in service" state for the ADSL port does not mean that the port carries customer service or that the port is cross-connected. It only means that the port is "operationally" or "administratively" in service. Since the NMS will perform the ATM cross-connection, it will be the system that will have the knowledge of DSLAM ports that carry customer service.

5.1.2 Dependencies

Based on the above note, DSLAM currently does not know which ports carry customer service. Hence, *the NMS that will provision the PVCs must indicate which ADSL ports are "in service" and the total count of ADSL ports that have been put into service* (see Section 7).

5.1.3 Feature Flow

Since capacity management is related to DSLAM ports, the only TL1 command needed is the "RTRV-ADSL" command, which identifies the "equipped" ports. It further specifies the associated operational and administrative states of each port. NMS should automatically and periodically issue this command to capture the equipped ADSL ports, including their administrative *and* operational status. This data should be stored in NMS and be used by the PVC management process (see the note below).

Grouping and ranging per AID are allowed for "RTRV-ADSL" command, hence, *NMS should also be able to obtain the total number of the "equipped" ports that are operationally and administratively in-service.* The equipped ports that are either operationally or administratively "out-of-service" should not be included in the total count since these ports are not available for service.

Note: When NMS receives the service orders from SOCS or implements a PVC through the GUI, it must check to ensure the assigned DSLAM port is administratively and operationally in-service. That is, a port that is administratively or operationally "out-of-service" should not be cross-connected by NMS. If a port is 'out-of-service," the NMS must issue an RMA (see Section 7).

5.1.4 Requirements (R1)

CAP-NMS-1 NMS shall track the following capacity related thresholds:

- **numberOfAvailableADSLPorts** - The total number of available ADSL ports (i.e., ports that are equipped, assignable, operationally and administratively in-service, and no cross-connect associated with them).
- **thresholdForAvailableADSLPorts** - NMS user-settable threshold for number of available ADSL ports. When "numberOfAvailableADSLports < thresholdForAvailableADSLports," NMS shall provide a capacity alert. This will be a trigger to populate the DSLAM with additional LT cards. In Release 1, this

will be a *global* threshold, that is, the user settable threshold will apply to all DSLAMs.

- **percentUtilizationDSLAMports** - Percentage of total DSLAM ports that are in-service (i.e., cross-connected). Currently the total DSLAM capacity is 576 ports.
- **thresholdForPercentageUtilization** - NMS user-settable DSLAM capacity utilization threshold. When "percentUtilizationDSLAMports > thresholdForPercentageUtilization," the NMS shall provide a capacity alert. This will trigger the appropriate capacity manager to start planning process for installation of a new DSLAM. In Release 1, this will be a *global* threshold, that is, the user settable threshold will apply to all DSLAMs.

CAP-NMS-2 NMS shall periodically issue the RTRV-ADSL command (with appropriate grouping and ranging) to retrieve information on all the "equipped" ADSL ports in each DSLAM. Furthermore, NMS shall note the ports' operational and administrative states. In particular, NMS shall note all the equipped ports that are administratively and operationally "in service." After each retrieval, NMS shall store such information and shall calculate the total number of "equipped and in-service" ports. Such information shall be stored in NMS for the past "n" days ("n" is a user-definable number with a maximum of 30 days).

CAP-NMS-3 When issuing the RTRV-ADSL command, NMS shall show (in a table format) all the equipped ports and the corresponding COSMOS and LFACS naming conventions for each equipped Alcatel port. This information may be used for trouble resolution when the NMS user communicates with COSMOS and LFACS users.

CAP-NMS-4 For each DSLAM, NMS shall provide from its database "real time" information on the total number of cross-connected ADSL ports. The NMS shall note this information every time a cross-connect is made and shall provide a history of the total number of "cross-connected" ports for the past "n" days ("n" is a user-definable number with maximum of 30 days). These numbers (or their differences) indicate "how fast" the DSLAM ports are cross-connected or put into service.

CAP-NMS-5 Upon each DSLAM ADSL port retrieval, NMS shall subtract the total number of ADSL ports that are cross-connected (i.e., INV-NMS-4) from the total number of equipped ports that are operationally and administratively "in service" (i.e., INV-NMS-1). This indicates the number of DSLAM ports that are available for assignment. If the difference is less than a user-definable threshold (e.g., 10), NMS shall automatically generate an alert. This threshold shall be checked during the processing of service orders for the FastAccess service. NMS shall keep a history of "available" DSLAM ports for the past "n" days.

CAP-NMS-6 If the percentage of the "cross-connected/in service" ports of a DSLAM becomes larger than %X (X being a user-definable number, e.g., 50) of the total capacity of DSLAM (i.e., 576 ports), NMS shall automatically generate an alert.

CAP-NMS-7 The NMS user shall be able to manually suppress capacity alerts through the NMS GUI. However, the capacity alerts should not be cleared until capacity gets replenished.

CAP-NMS-8 NMS shall provide per day total number of the ADSL ports (within each DSLAM) that have been cross-connected for the past "n" days.

CAP-NMS-9 NMS shall be able to provide reports on capacity alerts and information specified in the above requirements. Furthermore, NMS shall be able to electronically transmit these reports to an appropriate Capacity Manager or Capacity Management Center.

CAP-NMS-10 NMS shall check the operational and administrative state of the DSLAM ports, before a DSLAM cross-connect is made on such a port. If by checking the NMS database, it is found that the administrative or operational state of a port is "out-of-service," NMS shall not proceed with the cross-connection and shall issue an RMA to the NMS user.

CAP-NMS-11 For capacity management, the NMS user shall be provided with the capability to set and change the following global thresholds from the GUI screen:

- **thresholdForAvailableADSLPorts** - threshold for number of available ADSL ports
- **thresholdForPercentageUtilization** - threshold for DSLAM capacity utilization.

5.2 Retrieval of DSLAM Physical Inventory

5.2.1 Purpose

The purpose of this feature is to retrieve DSLAM physical inventory information and use the data to refresh the NMS database.

5.2.2 Dependencies

None.

5.2.3 Flow

- This feature may be initiated via on-demand request by NMS user or via NMS initiated automated periodic requests.
- Upon any of the above triggers, the NMS shall issue a retrieve inventory command.
- NMS will refresh its database and store the data, which may be used by other features (e.g., PVC provisioning).

5.2.4 Requirements (R1)

INV-NMS-1 NMS shall be able to retrieve the entire DSLAM inventory data, including physical and logical inventory data (for the logical inventory, see Section 7). The trigger may be an on-demand NMS user request or automated periodic request by NMS. NMS shall provide the user the capability to perform this task with one command for a specified set of TIDs (grouping and ranging per TID).

Note: The frequency of use of this feature should not be too often as it will impact NMS performance.

The following commands may be used to retrieve DSLAM physical inventory. These commands support grouping and ranging per AID:

- "RTRV-EQPT" command to retrieve installed and pre-provisioned equipment inventory.
- "RTRV-INV-EQPT" command to obtain all equipment inventory. This command provides additional information to the "RTEV-EQPT" command. For example, it provides the software release of the specified equipment (e.g., card).
- "RTRV-ADSL" command to provide a list of "equipped" ports with their appropriate operational and administrative states. This command is also used for DSLAM capacity management (previous feature).
- The RTRV-INV-EQPT command identifies the ATU-C cards, not the ports. The RTRV-ADSL command identifies the ports.
- "RTRV-VCL, RTRV-CRS-VC" (see PVC management section).

The command "RTRV-INV-EQPT" is recommended since it provides the important software release information. This software release information is needed for trouble-shooting purposes. For example, if an ATU-R does not "sync" with an ATU-C, it may be due to different software releases.

This physical inventory feature and the logical inventory feature (see Section 7) may be used together to retrieve the entire DSLAM inventory.

5.3 Selection of Next Available DSLAM Port (R2)

5.3.1 Purpose

In Release 1 of NMS, this function will be performed via COSMOS associated Halt programming. However, Halt programming provides a *static view* of DSLAM ports and if the operational or administrative states of a port are changed, Halt would not know about it. Hence, Halt may select a DSLAM port that is operationally or administratively out-of-service, causing NMS to RMA the service order. This is because COSMOS may assign a port that is not available for service.

In Release 4 of ADSL TL1 messages will be enhanced to provide an indication of which ADSL port is truly "in service" i.e., cross-connected. The current TL1 message only indicates which ADSL ports are "equipped" and state of the port as described in the above note.

The purpose of this feature to provide a "real time" (not static) view of the DSLAM and use it to select and reserve the next available port for assignment purpose. In this case, a port that is operationally or administratively "out of service" will not be selected. The DSLAM will provide this next available port with Alcatel naming convention. The NMS will provide a table to convert the Alcatel naming convention to the COSMOS naming convention.

5.3.2 Dependencies

This feature may be implemented depending on the availability of one of the following features:

- TL1 command line interface to support "next available port"
- CMISE command to support the same.

Note: The "next available port" feature will be available in ADSL R3.0, but such a feature will not be available in the TL1 interface. In Release 4 of DSLAM (3Q98), this feature will be available in both TL1 and CMISE interfaces.

5.3.3 Flow

- The feature may be initiated either by the NMS user or by the HAL system to help perform physical provisioning during the service activation process [1].
- When request for "next available port" is received at the NMS (via HAL or NMS user), the NMS will note the SO number and initiate appropriate command by identifying the TID for the DSLAM.
- The response to this command will provide a "next available port" and the DSLAM will change that port status to "pending". If a port is operationally or administratively OOS, that port will not be selected.
- The NMS translates the port Alcatel naming convention to the COSMOS naming convention and provides it to the initiator (the NMS user or HAL).

5.3.4 Requirements

TBD.

6. Service Order Management Requirements

6.1 Purpose

The purpose of this feature is to process FastAccess end-customer service orders, and report completions and failures to the NMS user. This function stores service orders for processing by NMS on the appropriate date and for reprocessing by the NMS user. An NMS user function to temporarily deny service (when requested by bill collection personnel) is also supported. This function provides the NMS user with capabilities to generate reports relating to service order activities and status. In summary, the purpose of this feature is to:

- Process end-customer FastAccess service orders
  - Use the contents of a FastAccess service order to determine service activity and customer information
  - Control service order processing (and reprocessing in the event of service order provisioning failure)
  - Maintain service orders and status
  - Create, change, or delete customer records
  - Interface with NMS PVC Management functions to set-up or tear-down PVCs.
- Provide an NMS user interface to deny (and restore) FastAccess service
- Provide an NMS user interface to manually reprocess a service order (in the case of a prior failure)
- Provide an NMS user interface to generate detailed and summary reports concerning service order activity and status.

6.1.1 Assumptions and Constraints

Service order writing procedures and SOCS will provide the required tags and data to flow end-customer orders through SOCS and NMS (using a SOCS Navigator Contract).

FastAccess services will be processed as change orders to an existing POTS service.

Service orders will reflect FastAccess new connects, disconnects, change orders (which could include deny and restore service), and record orders and updates (corrections) to pending orders (reissue before due date) for all of these service order types. For the initial offering of FastAccess service, a customer must have POTS service. FastAccess service will be processed via change order to the POTS service and disconnects the FastAccess service will also be processed as a change order to the POTS service. A disconnect order type will only be issued when the POTS service is being removed.

Record Orders with I and O action in the List section of the service order will be processed. Any I action for ADL in the S&E section of the service order will RMA.

Service Order type T and F will not be supported, and will RMA to be handled manually.

FastAccess service orders associated with remote DSLAMs will flow through the NMS in Release 1 and will be "RMA'd" for manual NMS processing.

FastAccess service changes will not be included in the flow-through process and will need to be handled manually in this release.

The BBOC is responsible for resolving all service order problems and resolving any failures. Notification of failures or problems will be reported to the BBOC NMS user, not back to SOCS. In addition, the BBOC will be responsible for handling all Change orders tp FastAccess services. Methods and procedures for processing Change orders for FastAccess service are undefined.

These requirements do not address flow-through support for physical link activation, such as NSP orders for DS3/OC3 interfaces to ATM to support FastAccess services. The Network Creation section of this document describes the NMS user interface for representing these physical links in NMS.

USOCs will exist to identify consumer and multi-tier business services. Service denial/restoration will be immediate, and may or may not have an associated service order.

6.2 Feature Description and Flow

6.2.1 Process Service Orders from SOCS

FastAccess service orders for end-customers will be sent from SOCS to NMS via a navigator contract interface (to be defined). The key features to be supported by NMS are:

- Parse FastAccess service orders to
  - Obtain customer information (customer telephone number [TN] to be used as the customer ID, customer name, and customer address).
  - Obtain service order activity (new connect, disconnect, change, record orders, or update (correction) for the supported order types).
  - Obtain USOC for class of service.
  - Obtain the due date.
  - Create a customer record (if one does not exist).
  - Store the service order (for an update (correction), overwrite the information for the matching order number; for new connects, disconnects, changes, and record orders, create a new object).

- If the order is for a new connect
  - Determine the due date and hold until 1 day prior to due date.
  - Determine the customer's serving DSLAM and assigned ADSL port from the COSMOS DSLAM assignment or the LFACS assignment on the service order. If LFACS assignment (for a remote DSLAM) for new service, RMA the order.
  - Determine if the ADSL port exists in the NMS. If it doesn't, the NMS shall notify the user and the service order shall be failed).
  - If the port exists, determine the type of PVC to be provisioned. This will be determined from the USOC on the service order and
    - ⇒ If it is a consumer service (category 1), a PVC from the DSLAM to Service Gateway will be established, using standard DSLAM profiles.
    - ⇒ If it is a business service (category 2), "best effort" class of service, a PVC from the DSLAM to the Service Gateway will be established, using standard DSLAM profiles.
    - ⇒ If it is a designed service (category 3), the three tiers of the designed services will all contain a circuit identifier of the physical link from the NSP to an ATM switch and the VPI and VCI to be used from the ATM switch to the NSP on the service order.
  - NMS will use the USOC to determine the appropriate ADSL profiles and ATM parameters to be used to provision the logical connections across the DSLAM and ATM subnetwork and reflect these in the customer's record.
  - If the order can not be completed successfully, NMS will generate a User Alert (RMA) to indicate the source of the problem and undo any logical connections, if any.
  - If the order is successful, NMS will:
    - ⇒ Check the status of the port to verify that it has no NMS alerts against it, then
      a) Generate a service order completion alert.
      b) Update the counters associated with DSLAM inventory.
      c) Determine if DSLAM inventory thresholds have been crossed and generate the appropriate alerts.
    - ⇒ Else generate a warning notification that the service order completed but the port is not in-service or has an outstanding alert.
- If the order is for a disconnect or cancellation of FastAccess service, NMS will:
  - Validate that the customer exists.
  - Determine the due date. Disconnects must be made on the due date.
  - On the due date, determine the DSLAM, the ADSL port, and the type of PVC to be disconnected from NMS database; use the appropriate NMS PVC functions to disconnect the FastAccess service.

If the order cannot be completed successfully, NMS will generate a User Alert (RMA) to indicate the source of the problem.

- If the disconnect order is successful, NMS will:
  - ⇒ Change the customer record indicate that the status is deleted.
  - ⇒ Generate a service order completion alert.
  - ⇒ Update the counters associated with DSLAM inventory.
  - ⇒ Determine the status of DSLAM inventory thresholds and any associated threshold crossing alerts, should be removed.

- If the order is for a FastAccess service change, the NMS will store the order and make it as pending. No further processing will be done on change orders in Release 1. Change orders will be processed manually and may be manually marked completed by an NMS user.
- If the order is a correction order (changes made to the order before the due date), the NMS will replace the information on the matching service order number with the current information).
- If the order is a Record order, it will be used to deny or restore service.
- Report completion or failures to the NMS user.
- Maintain information about all pending service orders and their completion status.
- When issuing the completion order, include the assigned profile and store with the completion status.

6.2.2 Service Order Corrections

A service order can be corrected at any time prior to the due date. Correction will have the original service order number. NMS shall determine if an order is a correction and if so, delete the original order and store the new, corrected order.

6.2.3 Deny and Restore Service

NMS capability to enable an authorized NMS user to deny (and restore) service is supported. This is to be used in the case when service is to be temporarily suspended, without removing all physical and logical connections. To accomplish this, the NMS user will be provided with an interface to deny (or restore) service, specifying the customer's ID. NMS will determine the DSLAM assignment for the customer and communicate with the DSLAM using the TL/1 interface with the command to change the operational status of the ADSL port to out-of-service (for denial) or in-service (for restoration of service). A change order can be issued to deny (suspend) or restore service. NMS should recognize this type of order and process as flow-through, updating the status of the customer record.

6-4

6.2.4 Reprocessing a Service Order

The NMS user will have the capability to reprocess a service order (in the case of a previous failure).

6.2.5 Service Order Management Reports

The NMS User will have reporting capabilities to summarize service order activity including:

- A summary (list and count) of completions and failures for a given date
- A list of failures to be reprocessed
- A list of customers denied service
- A summary of service orders to be processed on a particular date.

6.3 Release 1 Requirements

6.3.1 SOCS Interface (R1)

The SOCS interface will be used to flow a service order for end-customer FastAccess service to NMS for mechanized DSLAM port and PVC provisioning. This interface will be supported by a SOCS Navigator Contract Interface (see Section 11).

SOM-NMS-1 NMS shall parse the following information from the service order through a navigator contract interface to SOCS, as the first step in provisioning a new, disconnect, change, or corrections to a FastAccess service request. The information to be parsed is as follows:

Service Order Information:

- Service Order Number
- Service Order Type (new connect, change, disconnect) and updates (corrections) and cancels to any of these.
- Due Date
- SOCS Order Status (CP=Completion, CA=Cancel, PD=Pending).

Customer Information (from the listing section):

- Customer Name
- Customer Address (serving address (SA FID)).

Service Information (from the S&E section)

- USOC
- Telephone number (TN FID)
- VPI/VCI (for Category 3 services only)
- NSP.

Assignment Information (from the ASGM section)

- DSLAM and ADSL port assignment (in the OE section).

SOM-NMS-2 If NMS is unable to parse the service order and obtain the information from SOM-NMS-1 above, a service order Alert, SO-FAILED shall be generated for the NMS user, indicating the description that parsing was the reason for failure and service order number (if available).

SOM-NMS-3 NMS shall create a customer record (if one doesn't exist) if the service order can be parsed.

SOM-NMS-4 NMS shall keep a record of all service orders and status (completed, pending [new connect, disconnect, change, record], corrected, failed, and reason for failure). Multiple completed orders may exist for a single customer. NMS shall keep only the most recent version of a corrected service order.

A service order may be classified as pending and failed.

Open Issues:
Always keep current completed order, the current pending order and current status of pending order (e.g., if failed)

Once the pending order is completed, change the status from pending to completed and retain the order. Find out the implications of the record order on this flow. Is it complete and if not, may need to save 2 orders.

Do you keep status on completed disconnect orders??, if so, how long

SOM-NMS-5 NMS shall determine the customer's DSLAM and ADSL port assignment from the COSMOS assignment information on the service order for a new connect.

Open Issues:
How to determine the CO or site location? COSMOS uses the NPA NXX to determine the site location. NMS will need a relationship between the NPA NXX in the fielded Header section of the service order and the CLLI of the DSLAM equipment.

Table 6-1 illustrates DSLAM assignments and naming conventions. The current method evolved during the market trial (documented in the DCSC Method and Procedures). An example of the COSMOS name in the assignment (ASGM) section of a service order is "DSL14003-01-103." The DSL14003-01 describes the equipment and its physical location. The last three characters, "103" define the card and port. The first two characters define the Splitter card and the last digit defines the port. The "DSLAM port" refers to the LIM (LT) card. Because of the two NT slots to the left of the LT cards, the DSLAM card number in COSMOS is two larger than the corresponding LT card number

6-6

in the DSLAM . For example, the "10" refers to LT 8. The last digit in both entries refers to Port 3 (i.e., 103 in COSMOS would translate to slot 8, port 3).

Table 6-1. DSLAM Assignment Table and Naming Conventions

Office	CLLI	DSLAM
Homewood	BRHMALHW	DSL13007-01-031 ; DSL13007-01-144

Character	Identifies
First 3	The facilities as "DSL"AM equipment
Next 5	The Aisle and RELAY RACK of the DSLAM bay
Next 2	The bay SHELF holding the DSLAM equipment
Next 2	The CARD, numbered 03 through 14
Last 1	The CARD PORT, numbered 1 through 4

The Relay Rack and Bay may be the MDF termination.

During Network Creation of the DSLAM, the NMS user will input the physical rack information of the DSLAM system in the Rack fields (1-4 for Alcatel) provided on the user screen.

The rack always starts with 1 in Alcatel and the shelf always starts with 1 in Alcatel. Assume that the shelf will be the same.

SOM-NMS-6 NMS shall save but not process FastAccess service - new connects if the assignment is for a remote DSLAM. NMS shall determine this by the absence of the COSMOS assignment information and the presence of "PG" in the F1 field CA FID of the assignment section. NMS shall generate the SO-FAILED alert, indicating in the description that the order is a new connect Fast Access service associated with a remote DSLAM. The Assignment section shall be saved with the service order.

SOM-NMS-7 NMS shall save the service order and determine if the service order may be processed immediately or must be held for processing on a later date. These shall be stored as pending and NMS shall generate the SO-PENDING alert for these orders. NMS shall process FastAccess disconnect orders on the due date, FastAccess new connect orders one day prior to the due date, FastAccess updates (corrections to existing orders) will update the original order immediately, FastAccess record orders will be processed on the due date (only the List section will be processed, if an "I" action for

ADL is found in the S&E section, NMS will RMA the order) and FastAccess service change orders (changes) will be saved for manual processing.

For FastAccess service, new connects and disconnects, the following requirements apply.

SOM-NMS-8 NMS shall determine if the ADSL port exists in the NMS. If it does not exist, the SO-FAILED alert shall be generated. The alert description shall indicate that the ADSL port does not exist in the NMS.

SOM-NMS-9 NMS shall determine the type of PVC to be established or torn down. NMS shall use the class of service on the service order (as indicated by the USOC, USOCs still to be defined, Q4R to be used temporarily for Consumer) and determine the provisioning methodology as follows:

- If it is a service order FastAccess Consumer service, a PVC from the DSLAM to Service Gateway shall be established, using standard DSLAM profiles.
- If it is a Business service, "best effort" class of service, a PVC from the DSLAM to the Service Gateway will be established, using standard DSLAM profiles.
- If it is a Business designed service, the following procedure will be used:
  - The three tiers of the Business designed services will all contain a circuit identifier of the physical link from the NSP to an ATM switch and the VPI and VCI to be used from the ATM switch to the NSP on the service order.
- NMS will use the USOC to determine the appropriate ADSL profiles and ATM parameters to be used to provision the logical connections across the DSLAM and ATM subnetwork.

SOM-NMS-10 A request made by NMS for creation, deletion, or change of an ATM logical connection may fail. When NMS encounters such a failure, NMS shall roll back any created subnetwork connections and network link assignments from its database and request the DSLAM and ATM subnetwork to delete the corresponding subnetwork connection(s). The SO-FAILED alert shall be generated and the service order status shall be marked as failed. Failures associated with establishing logical connections are defined in Section 7.

In disconnecting a service, the end-to-end ATM logical connection(s) is removed. NMS shall support the following functions

SOM-NMS-11 NMS shall update a customer record with the selected ADSL and ATM profile information upon the completion of a service order.

SOM-NMS-12 NMS shall support a Navigator contract interface to SOCS to disconnect FastAccess service.

SOM-NMS-13 NMS shall parse the service order information received from the Navigator contract, determine the FastAccess service to be disconnected (consumer or business) and the customer ID. NMS shall retrieve from its database the customer's

assigned DSLAM, ADSL port, and the type and termination point of the PVC (an NSP or Service Gateway).

SOM-NMS-14 NMS shall use the PVC management functions to delete the PVC connections for the customer and set the state of the DSLAM ADSL port available for assignment. If NMS encounters a failure in deleting the PVC connections for the subscriber, NMS will generate the SO-FAILED alert and indicate the source of the failure on the alert description.

SOM-NMS-15 If no failures are detected, NMS shall delete the consumer customer record and notify the NMS User of successful completion of the service order. All other alerts associated with the order shall be cleared. Business customer records shall be retained for a period x days.

To deny (suspend) or restore service, the following capabilities shall be supported

SOM-NMS-16 NMS shall provide the NMS User an interface to deny (suspend) or restore service for a given FastAccess subscriber. Only authorized users shall be permitted to use these two functions. The NMS User will identify the subscriber by the customer ID (i.e., the TN).

NMS shall also support the processing of a change order to deny (suspend) and restore function. *(Add the format and FIDS to look for. This is an open item.)*

SOM-NMS-17 NMS shall use the specified customer ID to retrieve the DSLAM assignment for that customer. Using the TL/1 interface to the DSLAM, NMS shall issue the ED-ADSL command as follows:

ED-ADSL:[tid]:aid-adsl:[ctag]:::[pst];

where

tid = the DSLAM identifier for TL/1 interface
aid-adsl = the full name of the DSLAM port assigned to the customer in the form of ADSL-rack-shelf-lt_slot-circuit
ctag = a command correlation tag for the response
pst = OOS for Out-Of-Service (deny) or IS for In-Service (restore).

SOM-NMS-18 NMS shall parse the response for the ED-ADSL command. If the response is COMPL and the request is to deny service, an alert shall be generated indicating to the NMS user that service was successfully denied to the customer (the customer ID and action). In addition, the customer record shall indicate if service has been denied and the date that it was denied. If the response is COMPL and the request was to restore service, NMS shall clear the alert to deny service and generate an alert that service was successfully restored to the customer.

If the response to the ED-ADSL command indicated and error (i.e., DENY was returned) an alert shall be generated indicating to the NMS user that the request to deny or restore failed and the customer ID. The returned error code and description of the code shall also be included on the alert.

To quickly reprocess failed service orders, the following requirement is needed

SOM-NMS-19(O) NMS shall provide the NMS user an interface to reprocess a service order. The NMS user shall provide the number of the service order to be reprocessed. If the service order processes successfully, NMS shall clear the failure notification for the service order.

To provide reports concerning service order activity and status, the following capabilities will be supported.

SOM-NMS-20(O) NMS shall provide an NMS user interface to generate reports and summaries of service order activities including:

- A summary (list and count) of completions and failures for a given date
- A list of failures to be reprocessed
- A list of customers denied service
- A summary of service orders pending to be processed, by their due date.

SOM-NMS-21 Service order processing alerts shall be classified as service order alerts. The alerts generated are as follows:

NMS unable to parse pending SO

Alert Name SO-COMPLETED

Description:	Service Order successfully completed {SO number, TN}
Affected Object:	Customer ID
Severity:	Indeterminate (magenta)
Caused By:	Successful completion of a service order
Cleared By:	Manual Clear
Causes and Actions:	All customers supported by card are affected.

Alert Name SO-FAILED

Description:	Service order failed {reason for failure}
Affected Object:	Customer ID
Severity:	Critical

Caused By:	Failure to parse SO, ADSL port unknown to NMS, PVC provisioning failure.
Cleared By:	SO-COMPLETED or Manual Clear
Causes and Actions:	All customers supported by card are affected.
Reason for Failure:	Service Order type not supported
	Unable to parse COSMOS assignment
	USOC unknown
	Unable to parse LFACS DPG/Pair assignment
	Unable to determine site location

Alert Name SO-PENDING

Description:	The Service order is being held until processing date {customer ID, Due date}.
Affected Object:	Service Order number
Severity:	Indeterminate (magenta)
Caused By:	Card going down. Provide Switch ID/Card ID.
Cleared By:	SO-COMPLETED or SO-FAILED alert
Causes and Actions:	The service order is being held until the appropriate processing date.

6.3.2 Questions/Issues

If the disconnect is for a Business service, should NMS RMA the order? The NMS User may need to call the customer to verify if the disconnect should be processed. If the answer is yes, reenter into the service order process flow. If no, customer should make a request to correct the order.

Disconnect orders for Consumers should follow the normal service order process flow. Maintaining the completion status of a disconnect order? If so, for how long? (e.g., 2-3 days after due date)

Format and FIDS associated with a change order for restoration or denial of service are to-be-defined.

The format for all business service orders are to-be-defined.

All USOCS are to be defined (only a temporary USOC for consumer service exists). How to determine the CO (site location) of a COSMOS-assigned DSLAM.

7. PVC Management

7.1 Purpose

The purpose of this feature is to provision PVCs (VCCs and VPCs) and manage their inventory to support the FastAccess service. This feature will

- Provide a user interface to create, delete, change, and retrieve PVCs (VPCs and VCCs)
- Provision PVCs through the service order flow for FastAccess services.
  - Use the contents of a FastAccess service order to determine service activity, PVC end-points, and PVC parameters such as quality of service.
  - Interface with the DSLAMs using a TL/1 interface and with the ATM subnetwork using NavisXtend Provisioning Server to create, change, or delete PVCs
- Manage the inventory of PVC (VCC and VPC) assignments
  - Discover/retrieve ATM PVC assignments and cross connections from DSLAMs using the TL/1 interface and from the ATM subnetwork using the NavisXtend Provisioning Server SNMP interface and refresh NMS logical inventory.

7.1.1 Dependencies

PVC management and provisioning is dependent on

1. The availability of network resources established by Network Creation including physical links and termination points to support PVC provisioning and Fault Management, which maintains a view of the status of network resources, a part of which may play a role in PVC assignment, such as the availability of the DSLAM TL/1 interface and NavisXtend Provisioning Server SNMP interface (and associated communication interfaces).
2. Ascend's NavisCore will be used to provision
   - Switch configurations (equipment holders, circuit packs)
   - Physical ports terminating FastAccess service physical links on the ATM subnetwork.
3. Alcatel's AWS will be used to provision
   - DSLAM configurations (equipment holders)
   - ADSL and ATM profiles
   - DSLAM - ATM Network Interfaces on the DSLAM (the OC3/DS3 interface NT).
4. Service Gateway functions are to be defined. Since the Service Gateway can have up to five physical interfaces to the ATM subnetwork, it is assumed that the NMS user will be able to associate the physical termination for each of the physical links.

7.1.2 Assumptions and Constraints

All PVC management for FastAccess services will be done through NMS only[4] (i.e., not through the supplier EMS GUI). PVC connections created on AWS or NavisCore will not be automatically detected by NMS. However, NMS will support the retrieval of PVCs for all ports associated with FastAccess services and loading of this PVC inventory into NMS.

Configuration of ATM physical ports will be done through NavisCore. Therefore, NMS will use a User Interface[5] to create FastAccess associated ATM ports.

PVC modifications (e.g., increase/decrease bandwidth, change VPI/VCI) to an existing PVC will be supported. However, specific changes have not been defined for the service. Hence, this document does not describe NMS requirements relating to PVC changes.

It is assumed that DSLAMs and the ATM network can support a VCI range of 101 to 677. This will enable the existing trial method and procedures to determine the VCI for a DSLAM connection from an ADSL port (a circuit on an LT) to the DSLAM OC3 port (the NT) based on the position of the ADSL port within the DSLAM.

7.2 Feature Description and Flow

7.2.1 Alcatel Profiles

Alcatel uses profiles to set up the ports (NT and ADSL) and the PVCs. There are four types of profiles: ADSL, ATM Access Control (ATMACC), Call Admission Control (CAC), and Traffic Descriptor (TRAFDSC). These profiles will be created using the AWS (not by NMS) and a subset of the profiles will be standard across all DSLAMs for service provisioning by NMS. When creating the profiles, a name is given as well as a number but the number is used when provisioning a port (or VCL/VPL). There can be up to 10 ADSL profiles (1-10) and up to 20 profiles for each of the ATMACC, CAC and TRAFDSC profiles (1-20).

When provisioning the end-customer with service on a DSLAM, three of the profiles must be specified at the port level (ADSL, CAC and ATMACC). In addition, the profiles need to be specified for the upstream and downstream for the CAC. There is a distinction made in the documentation (ED-ADSL command) about setting CAC profiles for ADSL Fast Channel and ADSL Interleaved Channel. Interleaved was intended for

[4] This assumes that the conversion to NMS is completed and that all FastAccess manageable resources and PVCs are inventoried in NMS.

[5] Other alternatives will continued to be explored to eliminate manual entry into NMS. One alternative is to identify the ports in NavisCore as FastAccess related. A process could then be developed to retrieve all ATM physical ports and determine those related to FastAccess service. A second alternative may use a TIRKS query to extract FastAccess circuits and ATM port terminations.

video so a single default value can be specified. The Fast Channel ADSL profiles will need to be used for FastAccess service.

A profile cannot be changed if PVCs have been provisioned across the port. As a result, any service change that requires the profiles to change will require that the existing VCC be deleted before the new service is created (Release 2 feature).

When provisioning a VCC across the DSLAM (using the ENT-VCL command) on either the NT or ADSL port, the TRAFDSC profile is specified for the receive and transmit directions. The PVC is completed by the ENT-CRS-VC command which has no profiles associated with it (it performs the logical connection between the ADSL port VPI/VCI created by ENT-VCL and the NT VPI/VCI, also created by the ENT-VCL).

7.2.2 Ascend PVC Provisioning

ATM parameters associated with ATM VCCs and VPCs are under study.

7.2.3 PVC Provisioning

For logical ATM connections, a PVC is an end-to-end ATM logical connection (either a VCC or VPC). The VPI and VCI assignments are the ATM cell header of a PVC are significant only to a specific ATM interface (i.e., the NSP UNI, DSLAM-ATM interface) and may be changed at multiplexing (i.e., the DSLAM) and switching points in the network (i.e., the ATM subnetwork and Service Gateway). To establish a PVC in the network supporting FastAccess services, the following steps apply to both Alcatel and Ascend:

1. Determine the DSLAM or ATM switch and physical ports to be used as the termination points of the PVC. For the DSLAM, one point will be the ADSL port and the network termination (NT) interface to the ATM subnetwork (a physical OC3 or DS3 link). For the ATM subnetwork, two physical ATM ports will be specified.
2. For each port terminating the PVC, logical ports must be created, specifying the VPI and VCI values for the PVC at each termination point.
3. A cross-connection is then made between the two logical terminations.

Four types of FastAccess service ATM VCC or VPC connections will be supported by this feature:

1. Within the ATM subnetwork, a Virtual Path Connection (VPC) will be established between the ATM subnetwork port associated with the Service Gateway physical link termination and the ATM subnetwork port associated with the DSLAM physical link termination as shown in Figure 7-1. The assumptions are
   - Network creation processes drive this activity whenever a new DSLAM or Service Gateway is added to the network

- An DSLAM is connected to only one Service Gateway; thus only one VPC will be needed between a DSLAM and Service Gateway. A Service Gateway may support multiple DSLAMs.
- A NMS User Interface will be used to identify the ATM subnetwork physical ports, the VPI at each end of the VPC. NMS will create within its data base, as needed, the physical and logical port terminations for the VPC.
- NMS will create the logical ports and ATM subnetwork connection (i.e., the VPC) for each of the physical ATM subnetwork ports.
- A PVC-ID will be generated by NMS for this VPC as specified in G-NMS-9 (DSLAM CLLI-SERVICE GATEWAY CLLI-VPI at DSLAM).

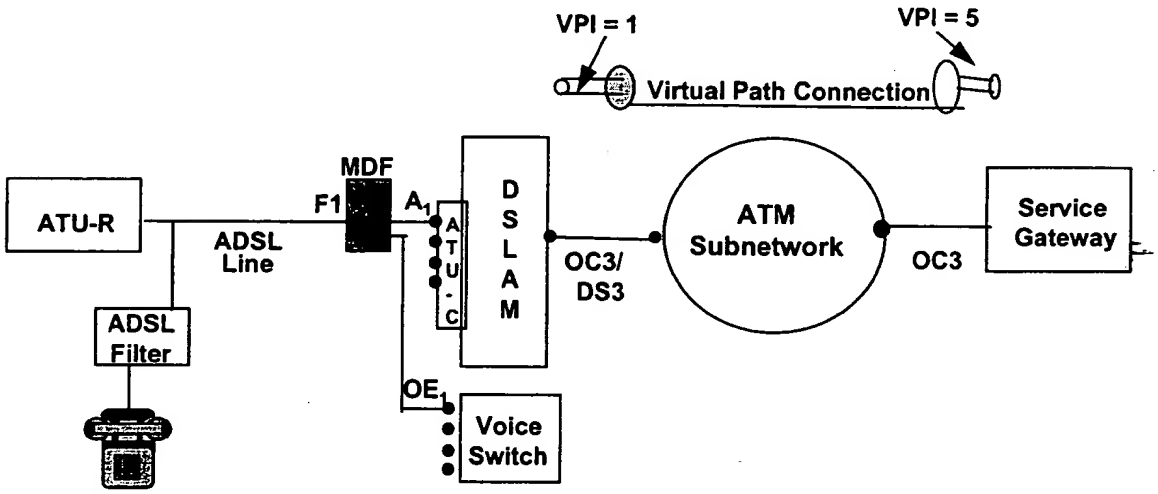

Figure 7-1. Virtual Path Connection from DSLAM to Service Gateway - Resource Provisioning

2. For FastAccess end-customers connecting to an NSP with a class of FastAccess service that establishes the connection via the Service Gateway, a PVC/VCC from the ATU-R to the Service Gateway will be established (or removed) as shown in Figure 7-2. The assumptions are
   - A service order or NMS User (reprocessing a service order) will initiate this process.
   - The ATU-R will be pre-provisioned with default VPI/VCI.
   - For the OC3/DS3 port of the DSLAM, the customer's assigned ADSL port and its position in the DSLAM will be used to determine the VCI. The VPI will be determined from the VPC pre-established from the DSLAM to the Service Gateway. NMS will use Alcatel's TL/1 commands to provision the logical port on the NT port. On the ADSL port, the ADSL profiles corresponding to the class of service will be provisioned. The ADSL port may have factory installed standard VPI/VCI. If this is not the case, the logical port must be provisioned using a predetermined VPI/VCI. The TL/1

command to cross-connect these 2 logical (at the ADSL port and NT port) end points must then be done.

- The VPC from the DSLAM to the Service Gateway will exist and will not require that the VCC within the VPC on the ATM subnetwork be provisioned.
- NMS will generate a unique PVC ID for this connection as specified in G-NMS-9 (TN-VPI-VCI of the ADSL access link).

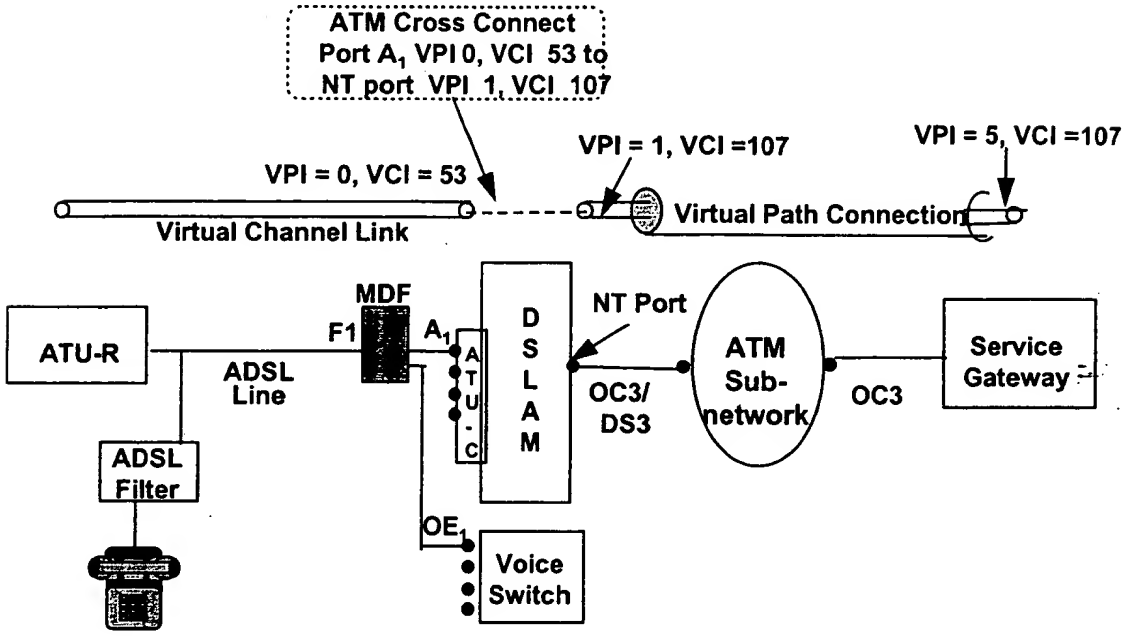

Figure 7-2. End Customer PVC to Service Gateway

3. A USOC will be used to determine if a FastAccess end customer is to be connected directly to a Corporate LAN and a VCC will be provisioned across the DSLAM and ATM subnetwork as shown in Figure 7-3. The assumptions are
   - The ATU-R will be pre-provisioned with default VPI/VCI.
   - NMS will use the TL/1 interface to provision the ADSL port with the profiles associated with the class of service.
   - NMS will use the TL/1 interface to provision the NT port and the ATM cross-connection on the DSLAM from the ATU-R input on the ADSL port and select a unique VPI/VCI to be carried over the NT interface (selection algorithm to be determined).
   - The NSP circuit ID will be specified on the service order and will be used to determine the NMS physical link for the NSP.
   - NMS will use the NavisXtend Provisioning Server SNMP interface to provision the ATM cross-connection from the ATM port associated with

DSLAM's ATM physical link termination (using a unique VPI) and the ATM port associated with the NSP ATM physical link termination.

- The VPI/VCI to be used at the NSP ATM port will be specified on the service order.
- NMS will generate a PVC-ID for this VCC per G-NMS-9 (TN-VPI-VCI of the ADSL access).

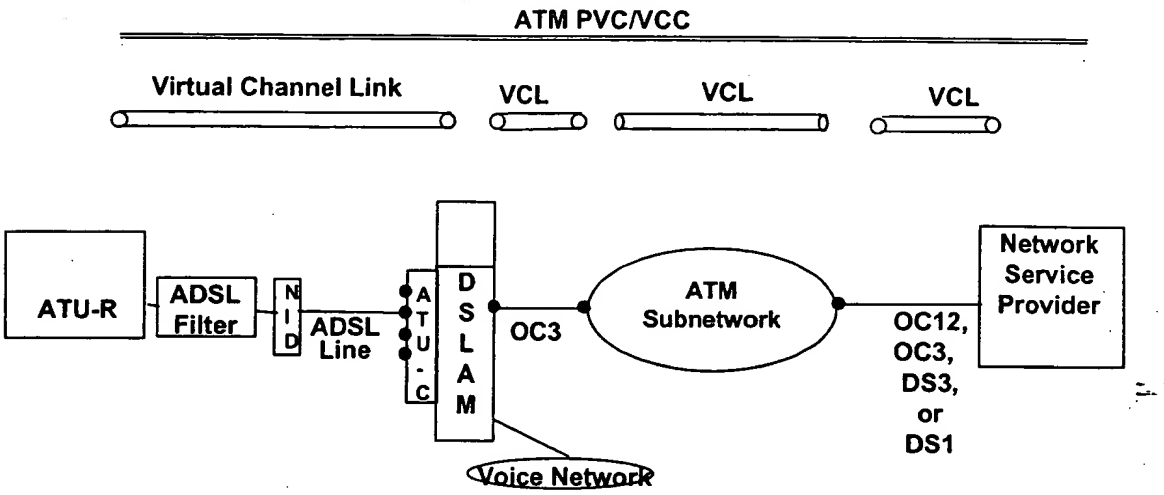

Figure 7-3. End Customer PVC to Corporate LAN

4. To support Network Creation, NSPs supporting FastAccess services via the Service Gateway will need a VCC to be established across the ATM Subnetwork from the NSP ATM physical link termination (i.e., that ATM port) to the Service Gateway ATM link termination (the ATM port) as shown in Figure 7-4. The assumptions are
   - This process may be driven by a service order (designed special order) for both the physical interface to the NSP as well as an NSP PVC order for FastAccess connectivity. The format of these orders and uniqueness for FastAccess are to-be-determined.
   - The NSP may specify the a pool of VPI/VCIs to be used at the NSP ATM termination point to provision the logical port.
   - NMS will generate a PVC-ID for this connection per G-NMS-9 (Service Gateway CLLI-NSP Circuit ID).

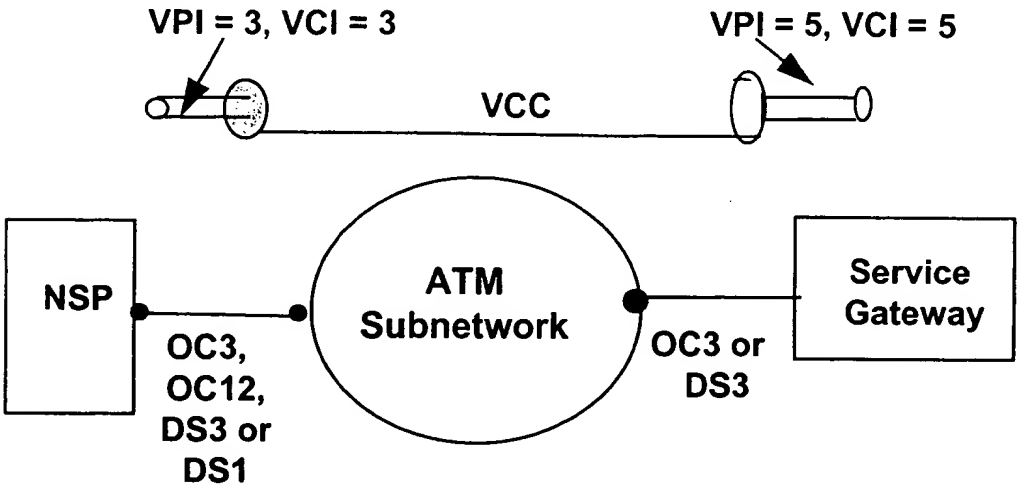

Figure 7-4. VCC from NSP to Service Gateway

7.3 Release 1 Requirements

7.3.1 PVC Provisioning (R1)

The following capabilities must be accessible via both the GUI and an interface to SOCS

PVC-NMS-1 NMS shall support the provisioning of both ATM Virtual Channel Connections (VCCs) across the DSLAM and ATM subnetwork and ATM Virtual Path Connections (VPC) across the ATM subnetwork.

PVC-NMS-2 NMS shall provision ATM logical connections required to support all the FastAccess classes of services and corresponding profiles on a DSLAM. Examples of the types of profiles to be set for each FastAccess class of service and the profile names are summarized below. Profile numbers (not names) must be used in the TL/1 command. The numbers are to-be-defined.

SERVICE PROFILE FORM: Consumer Services (Tiers 1 and 2)	
DESCRIPTION	**VALUE**
General	
Service Profile Identification - Profile Label (1 Per Service)	ADSL_CONS.nw
QOS Class - Quality of Service - Constant Bit Rate	NA
QOS Class - Quality of Service - Unspecified Bit Rate	UBR
Profiles - ADSL Line Profile	dn1200_up154.nw
Profiles - ATM Access Profile	ATM_cons.nw
Profiles - Upstream CAC Profile	CAC_up_cons.nw
Profiles - Downstream CAC Profile	CAC_down_cons.nw
VC Connections	
Connection - Number of VC Connections	
Virtual Connection Links - Network to User ATM Traffic Descriptor	UBR64.nw, UBR1000.nw
Virtual Connection Links - User to Network ATM Traffic Descriptor	UBR64.nw UBR1000.nw

SERVICE PROFILE FORM: Business Best Effort	
DESCRIPTION	**VALUE**
General	
Service Profile Identification - Profile Label (1 Per Service)	ADSL_BU_BE.nw
QOS Class - Quality of Service - Constant Bit Rate	NA
QOS Class - Quality of Service - Unspecified Bit Rate	UBR
Profiles - ADSL Line Profile	dn1200_up461.nw
Profiles - ATM Access Profile	ATM_Bus_be.nw
Profiles - Upstream CAC Profile	CAC_up_Bus_be.nw
Profiles - Downstream CAC Profile	CAC_down_Bus_be.nw
VC Connections	
Connection - Number of VC Connections	
Virtual Connection Links - Network to User ATM Traffic Descriptor	UBR64.nw, UBR1000.nw
Virtual Connection Links - User to Network ATM Traffic Descriptor	UBR64.nw UBR1000.nw

SERVICE PROFILE FORM: Business Service Tier 1	
DESCRIPTION	**VALUE**
General	
Service Profile Identification - Profile Label (1 Per Service)	ADSL_BUS_1.nw
QOS Class - Quality of Service - Constant Bit Rate	NA
QOS Class - Quality of Service - Unspecified Bit Rate	CBR
Profiles - ADSL Line Profile	dn1800_up461.nw
Profiles - ATM Access Profile	ATM_Bus_1.nw
Profiles - Upstream CAC Profile	CAC_up_Bus_1.nw
Profiles - Downstream CAC Profile	CAC_down_Bus_1.nw
VC Connections	
Connection - Number of VC Connections	
Virtual Connection Links - Network to User ATM Traffic Descriptor	CBR64.nw, CBR1000.nw
Virtual Connection Links - User to Network ATM Traffic Descriptor	CBR64.nw CBR1000.nw

SERVICE PROFILE FORM: Business Services Tier 2	
DESCRIPTION	**VALUE**
General	
Service Profile Identification - Profile Label (1 Per Service)	ADSL_Bus_2.nw
QOS Class - Quality of Service - Constant Bit Rate	NA
QOS Class - Quality of Service - Unspecified Bit Rate	CBR
Profiles - ADSL Line Profile	dn1800_3600_up461.nw
Profiles - ATM Access Profile	ATM_Bus_2.nw
Profiles - Upstream CAC Profile	CAC_up_Bus_2.nw
Profiles - Downstream CAC Profile	CAC_down_Bus_2.nw
VC Connections	
Connection - Number of VC Connections	
Virtual Connection Links - Network to User ATM Traffic Descriptor	CBR64.nw, CBR1000.nw
Virtual Connection Links - User to Network ATM Traffic Descriptor	CBR64.nw CBR1000.nw

SERVICE PROFILE FORM: Business Service Tier 3	
DESCRIPTION	**VALUE**
General	
Service Profile Identification - Profile Label (1 Per Service)	ADSL_Bus_3.nw
QOS Class - Quality of Service - Constant Bit Rate	NA
QOS Class - Quality of Service - Unspecified Bit Rate	CBR
Profiles - ADSL Line Profile	dn3600_7000_up461.nw
Profiles - ATM Access Profile	ATM_Bus_3.nw
Profiles - Upstream CAC Profile	CAC_up_Bus_3.nw
Profiles - Downstream CAC Profile	CAC_down_Bus_3.nw
VC Connections	
Connection - Number of VC Connections	
Virtual Connection Links - Network to User ATM Traffic Descriptor	CBR64.nw, CBR1000.nw
Virtual Connection Links - User to Network ATM Traffic Descriptor	CBR64.nw CBR1000.nw

PVC-NMS-3 NMS shall provision the ATM logical connections to support Fast Access classes of service across the ATM subnetwork. The attributes to be set and corresponding values to support these classes of services are to be defined.

PVC-NMS-4 NMS shall support a user interface to create and delete a PVC, given the PVC ID or a Customer ID.

PVC-NMS-5 NMS shall support a service order interface to create and delete PVCs.

PVC-NMS-6 NMS shall provide the NMS user with a circuit view of a PVC to a service gateway, with the sequence of NE cross-connections that make up the network connection. The PVC ID shall be supplied as input. The following information shall be displayed

- PVC ID
- Customer/DSLAM/Service Gateway ID
- ADSL and ATM ports
- ATM and traffic descriptor profiles
- VPIs across the DSLAM-ATM and ATM-Service Gateway interfaces.

PVC-NMS-7 As part of PVC activation/deactivation, NMS shall support an SNMP interface to the ATM subnetwork to create, change or delete PVCs. Examples of the SNMP interface to the NavisXtend Provisioning Server follow

Specifying the OID
To access a specific variable from a MIB group, enter an OID that uses the following format:

{Provisioning Server OID}.{Group}.{Sub-group}.{Table}.{Entry}.{Column}.{Index}

Complex objects, such as LPorts and circuits require a sub-group, simple objects do not.

The Provisioning Server OID is:

1.3.6.1.4.1.277.9

Example 1: get Command

To find out what type of card is located in a particular slot of a switch, use the following steps to determining the OID of the command you want to issue:

1. Determine the group value by locating the Card Group in the beginning of the MIB document. The following line indicates that the group value is **4**:

   card OBJECT IDENTIFIER : : = {psMibRev2 4 }

   Cards are simple objects that do not require a sub-group name.

2. Determine the Table value by locating the Table index, **cardTable**. The line **::= { card 1 }** indicates that the Table value is **1**:

   cardTable OBJECT-TYPE
   SYNTAX SEQUENCE OF CardEntry
   MAX-ACCESS not-accessible
   STATUS current
   DESCRIPTION
   "Table representing information about all cards in the network"
   : : = { card 1 }

3. Determine the Entry value by locating the Entry index, cardEntry. The line **::= { cardTable 1 }** indicates that the entry value is **1**:

Example 2 : get-next Command

To retrieve the Admin status for all LPorts on a switch, use the following steps to determine the OID of the command you want to issue:

1. Determine the group value by locating the LPort Group in the beginning of the MIB document. The following line indicates that the group value is **6**:

lportOBJECT IDENTIFIER : : = { psMibRev2 6 }

2. Admin status is a configuration attribute. To determine the Sub-group value, locate the LPortConfiguration table in the beginning of the MIB document. The following line indicates that the Sub-group value is **2**.

   lportConfiguration OBJECT IDENTIFIER : : = { lport 2 }

3. Determine the Table value by locating the Table index, **LportAdminTable**. The line
   ::= { lportConfiguration 1} indicates that the Table value is **1**:

lportAdminTable OBJECT-TYPE
SYNTAX SEQUENCE OF lportAdminEntry
MAX-ACCESS non-accessible
STATUS current
DESCRIPTION "List of logical port common attribute entries."
: : = { lportConfiguration 1 }

4. Determine the Entry value by locating the Entry index, **lportAdminEntry**. The line **::= { lportAdminTable 1 }** indicates that the Entry value is **1**:

lportAdminTable OBJECT-TYPE
SYNTAX LportAdminEntry
MAX-ACCESS non-accessible
STATUS current
DESCRIPTION
"Logical Port Configuration Entry"
INDEX { switchIdIndex, lportIfIndex }
: : = { lportAdminTable 1 }

5. Determine the Column value for the MIB variable you want to access. To retrieve the Admin status, you need to access the variable **lportAdminStatus**. The line
   ::= { lportAdminEntry 19 } indicates that Column value is **19**:

Example 3: set Command to Create an ATM LPort

To create an ATM LPort, use the vpiVciIndexTranslation table to map between the VPI/VCI pair and the LPort interface number. You must specify the LPort's VPI/VCI pair and request and interface number for that LPort.

To create an ATM LPort, use the following steps:

1. Issue an snmp_set request to obtain an LPort interface number based on the LPort's VPI/VCI pair. Set the vpiVciTransRowStatus to the createAndWait state, specifying the switchIdIndex 1.1.1.1, slotIdIndex 7, pportIdIndex 8, vpiIdIndex 2, and vciIdIndex 112.

   The SNMP agent processes the request and returns a successful snmpset_Response.

2. Issue an snmp_get request to obtain the interface number (lportIdIndex) that will be used to create a new entry in the lportAdminTable and the lportAtmTable. Issue the set request on the vpiVciIndexTransIfIndex, specifying the switchIdIndex, slotIdIndex, pportIdIndex, vpiIdIndex, and vciIdIndex values.

   The SNMP agent processes the request and returns an snmpest_Response with the lportIfIndex 7.

3. Issue a series of snmp_set requests that assign values to the attributes of the LPort in both the lportAdminTable and the lportAtmTable.

   The SNMP agent processes the requests by storing the values in the MIB cache. Then, the agent returns a successful snmpset_Response.

4. Issue an snmp_set request to commit the new entry. Set the lportAdminRowStatus to the active state, specifying the switchIdIndex 1.1.1.1 and the lportIfIndex 7. This command automatically sets the vpiVciIndexTransRowStatus to the active state.

   The SNMP agent processes the request by committing the new entry to the switch and to the NavisCore database.

   On receipt of noError messages from the switch and database, the SNMP agent returns a successful snmpset_Response to the MIB client.

Example 4: set Command to Create an ATM Circuit

To create an ATM circuit, define the two circuit endpoints using the atmCircuitEndpointTable and establish their interconnection using the circuitCrossConnectionTable.

To create a B-STDX ATM circuit, use the following steps:

1. Issue an snmp_set request to define the two circuit endpoints and establish their interconnection. Set the atmCircuitEndpointRowStatus to the

createAndWait state, specifying both endpoint 1 (switchIdIndex 1.1.1.1, slotIdIndex 7, vpiIdIndex 8, and vciIdIndex34) and endpoint 2 (switchIdIndex 2.2.2.2, slotIdIndex 4, vpiIdIndex 43 and vciIdIndex 54) in a single PDU.

The SNMP agent processes the request and returns a successful snmpset_Response.

2. Issue a series of snmp_set requests that assign values to the attributes of the circuit endpoints in the atmCircuitEndpointTable.

   The SNMP agent processes the requests by storing the values in MIB cache. Then, the agent returns a successful snmpset_Response.

3. Issue an snmp_get request to obtain the circuit number that will be used to create a new entry in the circuitCrossConnectTable. Specify the switchIdIndex, slotIdIndex, vpiIdIndex, and vciIdIndex values for one of the endpoints (the circuit number is the same for both endpoints).

   The SNMP agent processes the request and returns an snmpset_Response with the atmCircuitEndpointCircuitNumber 10.

4. Issue a series of snmp_set request that assign values to the attributes of the circuit interconnections in the circuitCrossConnectTable.

   The SNMP agent processes the requests by storing the values in MIB cache. Then, the agent returns a successful snmpset_Response.

5. Issue an snmp_set request to commit the new entry. Set the circuitCrossConnectRowStatus to the active state, specifying the atmCircuitEndpointCircuitNumber 10. This command automatically sets the atmCircuitEndpointRowStatus of the two endpoints to the active state.

   The SNMP agent processes the request by committing the new entry to the switch and to the NavisCore database.

   On receipt of a noError message from the switch and database, the SNMP agent returns a successful snmpset_Response.

Example 5: set Command to Delete an ATM Circuit

You can delete a circuit using either of the following methods:

* Specifying the circuit number.
* Specifying the circuit's endpoints.

Before deleting an object, perform a snmp_get request on the RowStatus attribute to check if another user is currently accessing the entry. If the entry is in use, retry your request later.

To delete an ATM circuit for which you know the circuit number, do the following:

Issue an snmp_set request to delete a circuit based on the circuit number. Set the circuitCrossConnectRowStatus to destroy the state, specifying the circuit number 10.

The SNMP agent processes the request by committing the new entry to the switch and to the NavisCore database.

On receipt of a noError message from the switch and database, the SNMP agent returns a successful snmpset_Response.

Example 6: set Command to Delete an ATM LPort

You can delete an LPort using either of the following methods:

* Specifying the interface number of the LPort
* Specifying the LPort's VPI/VCI pair.

Before deleting an object, perform an snmp_get request on the RowStatus to attribute to check if another user is currently accessing the object. If the object is in use, retry your request later.

To delete an ATM LPort for which you do not know the interface number, do the following:

Issue an snmp_set request to delete an LPort based on the LPort's VPI/VCI pair. Set the vpiVciIndexTransRowStatus to destroy the state, specifying the switchIdIndex 1.1.1.1, slotIdIndex 7, pportIdIndex 2, vpiIdIndex 2, and vciIdIndex 112.

The SNMP agent processes the request by committing the modified entry to the switch and the NavisCore database.

On receipt of a noError message from the switch and database, the SNMP agent returns a successful snmpset_Response.

To delete an ATM LPort for which the interface number is known, do the following:

Issue an snmp_set request to delete an LPort based on the LPort's interface number. Set the lportAdminRowStatus to the destroy state, specifying the switchIdIndex 1.1.1.1 and the lportIfIndex7.

The SNMP agent processes the request by committing the modified entry to the switch and to the NavisCore database.

On receipt of a noError message from the switch and database, the SNMP agent returns a successful snmpset_Response.

Example 7: set command to Modify an ATM LPort

You can modify a LPort using either of the following methods:

* Specifying the interface number of the LPort.
* Specifying the LPort's VPI/VCI pair.

Before performing a modification on any attribute, perform a snmp_get request on the RowStatus attribute to check if another user is currently accessing the entry. If the entry is in use, retry your request later.

Before modifying LPort attributes, set the vpiVciIndexTransRowStatus to the notInService state. You can skip this step if you specify the attribute modification in a single PDU.

To modify attributes of an ATM LPort for which you do not know the interface number, use the following steps:

1. Issue an snmp_set request to set the LPort to the notInService state, based on the LPort's VPI/VCI pair. Set the vpiVciIndexTransRowStatus to the notInService state, specifying the switchIdIndex 1.1.1.1, slotIdIndex 7, pportIdIndex 8, vpiIdIndex 2, and vciIdIndex 112.

   The SNMP agent processes the request and returns a successful snmpset_Response.

2. Issue an snmp_get request to obtain the interface number (lportIfIndex) that will be used to modify the entry in the lportAdminTable and the lportAtmTable. Issue the request on the vpiVciIndexTransIfIndex, specifying the switchIdIndex, slotIdIndex, pportIdIndex, vpiIdIndex, and vciIdIndex values.

   The SNMP agent processes the request and returns a snmpset_Response with the lportIfIndex 7.

3. Issue a series of snmp_set requests that modify values of the attributes of the LPort in both the lportAdminTable and the lportAtmTable.

   The SNMP agent processes the requests by storing the values in the MIB cache. Then, the agent returns a successful snmpset_Response.

4. Issue a snmp_set request to commit the modified entry. Set the lportAdminRowStatus to the active state, specifying the switch IdIndex 1.1.1.1 and the lportIfIndex 7. This command automatically sets the vpiVciIndexTransRowStatus to the active state.

   The SNMP agent processes the request by committing the modified entry to the switch and to the NavisCore database.

   On receipt of noError messages from the switch and database, the SNMP agent returns a successful snmpset_Response.

Example 8: set Command to Modify an ATM Circuit

You can modify an ATM circuit using either of the following methods:

* Specifying the circuit number.
* Specifying the circuit's endpoints.

Before performing a modification on any attribute, perform a snmp_get request on the RowStatus attribute to check if another user is currently accessing the entry. If the entry is in use, retry your request later.

Before modifying circuit attributes, set the circuitCrossConnectRowStatus to the notInService state. You can skip this step if you specify the attribute modification in a single PDU.

To modify attributes of attributes of a circuit for which you know the circuit number, use the following steps:

1. Issue an snmp_set request to set the circuit to the notInService state, based on the circuit number. Set the circuitCrossConnectRowStatus to the notInService state, specifying the circuit number 10.

   The SNMP agent processes the request and returns a successful snmpset_Response.
2. Issue a series of snmp_set requests that modify values of the attributes of the circuit. Modifications are made to the circuitCrossConnectTable and the atmCircuitEndpointTable.

The SNMP agent processes the requests by storing the values in MIB cache. Then, the agent returns a successful snmpset_Response.

3. Issue an snmp_set request to commit the modified entry. Set the circuitCrossConnectRowStatus to the active state, specifying the circuit number 7. This command automatically sets the atmCircuitEndpointRowStatus to the active state.

   The SNMP agent processes the request by committing the new entry to the switch and to the NavisCore database.

   On receipt of a noError message from the switch and database, the SNMP agent returns a successful snmpset_Response.

PVC-NMS-8 As part of PVC activation/deactivation, NMS shall support interfaces to the DSLAM to create, change or delete PVCs. The Alcatel TL/1 commands to provision a VCC are

- ED-ADSL (to establish the profiles on an ADSL port),
- ENT-VCL (to establish the VPI/VCIs at the ADSL port and NT port and set the traffic descriptor profiles) and
- ENT-CRS-VC to create the VCC from the ADSL port and the NT port.

The Alcatel TL/1 commands to delete a VCC are

- DLT-CRS-VC and
- DLT-VCL.

NMS shall not change the ADSL profiles if a VCC exists on the ADSL port.
NMS shall not change the Traffic descriptor profile on an existing VCC. The TL/1 command DLT-CRS-VC must be done first.

PVC-NMS-9 NMS shall provide the NMS user a reason or explanation if a PVC activation/deactivation request failed. The explanation will depend on the information provided by the Alcatel TL/1 and Ascend Provisioning Server SNMP interfaces. These include alerts indicating that the interface is not available, equipment is not available, duplicate PVC, or PVC does not exist.

PVC-NMS-10 NMS shall release all subnetwork connection transactions if a PVC network connection cannot be activated. In addition, NMS shall not retain that PVC ID in its network connection database.

PVC-NMS-11 NMS shall support a NMS User Interface to request the retrieval of subnetwork connections.
In setting up an end-to-end VPC or VCC network connection, NMS shall support the following functions.

PVC-NMS-12 NMS shall determine the VPI/VCI assignments if not specified on the service order or by the NMS User.

For DSLAM's NT port VPIs will be selected based on the destination of the service and the class of service.

- The VPI shall be 1 from the DSLAM NT port to the ATM network for the VPC connection to a Service Gateway.
- The VPI to be used to support connection from the DSLAM to a Corporate LAN will be predetermined and unique for that DSLAM-ATM network interface. A unique VPI may be selected (e.g., 10) and used for all service connections originating from the DSLAM and not terminating at the Service Gateway. The VPI and VCI to be used across the ATM-Corporate LAN interface will be specified on the service order.
- The VCI to be used for all services on a remote as well as central office DSLAM shall be determined based on the port location within the DSLAM. The calculation for the trial is currently

  100 + {[(rack-1)*3 + (shelf-1)]*12+(slot-1)}*4 + Port#.

  The range of VCIs is 101 to 677 using this algorithm.

  Alternatively, NMS may use a table to determine the VCI for a given port.

For the DSLAM's ADSL port (the LT and ADSL circuit), VPI/VCIs will be pre-installed and will be the same for every port on the DSLAM. The specific values are to be determined.

For the ATM connections, the VPI/VCIs for provisioning the logical ports are determined as follows:

- For services supported by a connection through the Service Gateway, a VPC will be pre-established as part of network creation/resource provisioning. The VCI assignments on the DSLAM will be unchanged in the ATM subnetwork at the DSLAM ATM link termination. The VPIs at either end of the VPC within the subnetwork where pre-established during the VPC provisioning process.
- For services not routed through the Service Gateway, at the ATM port terminating the interface to the DSLAM, the VPI/VCI used to provision the VCC across the subnetwork must be the same as the VPI/VCI selected for the DSLAM NT port.
- For services not routed through the Service Gateway, the selection of the VPI/VCI for the NSP ATM link termination will be specified on the end-customer's service order.
- For NSPs connected to a Service Gateway, VPI/VCI assignment guidelines at either end of the logical connection (VCC) are to-be-determined.

PVC-NMS-13 After NMS determines the VPI/VCI values for the termination points of a subnetwork connection, NMS shall request the subnetwork management system to set up a subnetwork connection between the selected termination points.

PVC-NMS-14 A request made by NMS to subnetwork for creation of a subnetwork connection may fail. When NMS encounters such a failure, NMS shall rollback any created subnetwork connections and network link assignments from its database and shall delete the corresponding subnetwork connection(s).

In disconnecting service and removing an end-to-end VPC or VCC connection, NMS shall support the following functions:

PVC-NMS-15 NMS shall support an NMS user interface and a SOCS interface (to be defined) to disconnect FastAccess service or delete specified VPC or VCC connections. Four separate scenarios shall be supported[6]:

1. Temporarily denying service (removing the DSLAM ADSL port from service) and administratively putting the customer's assigned port out-of-service.
2. Disconnecting service for a FastAccess end-customer based on the Customer ID
3. Removing a VPC between a Service Gateway and a DSLAM
4. Removing a VCC between a Service Gateway and a NSP.

PVC-NMS-16 NMS shall log PVC connection transaction completions and failures to a transaction log and shall indicate the source of the request (user input type or Service Order) and the reason for failure, if any.

7.3.1.1 PVC Provisioning: End-Customer to Service Gateway Flow

PVC-NMS-17 NMS shall retrieve and process FastAccess service orders on the appropriate date.

PVC-NMS-18 For new-connects, NMS shall determine the serving DSLAM, ADSL port and use the inventory of VPI/VCIs and assignment guidelines for the DSLAM Port and associated VPC to the Service Gateway, select and assign VPI/VCIs using an assignment algorithm used in the trial (see PVC-NMS-12).

PVC-NMS-19 NMS shall determine if the elements in the selected or pre-defined path (ATM subnetwork, DSLAMs, ATM and ADSL ports, physical links) are valid equipment. The user shall be notified if any equipment is unknown to NMS.

PVC-NMS-20 NMS shall issue the command for the DSLAM port provisioning (the ADSL profiles) and cross-connect and notify the user of completions/failures.

[6] Changes are not defined and are not included in this requirement.

PVC-NMS-21 NMS shall generate a PVC-ID for the connection from the DSLAM-ADSL port to the Service Gateway.

PVC-NMS-22 When a PVC is deleted, NMS shall delete the PVC across all network resources allocated to the network connection. All alerts associated with the PVC shall be cleared first.

Figure 7-5 illustrates this flow.

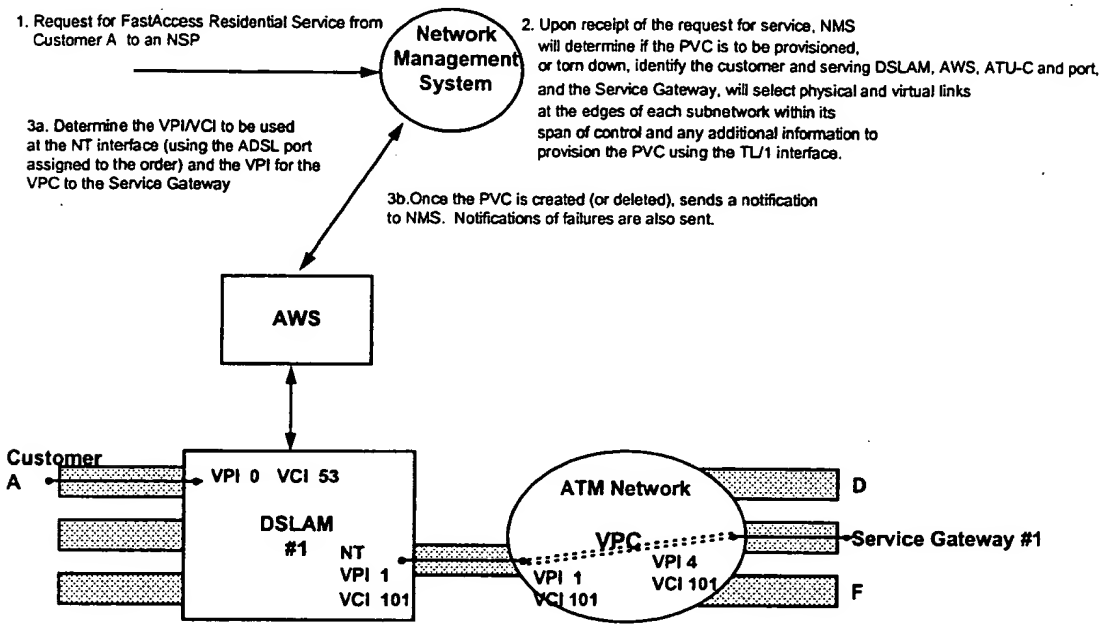

Figure 7-5. End-Customer to Service Gateway

7.3.1.2 PVC Provisioning: End-Customer to NSP Flow

PVC-NMS-23 NMS shall support a NMS User Interface to create (or delete) a VCC from an End-Customer to an NSP. The NMS User shall specify the

- The action (create or delete)
- The DSLAM and NSP Identifers
- The PVC ID and the Service Type (USOC)
- The VCIs to be used at each end of the VPC
- The VPIs to be used at each end of the VPC.

PVC-NMS-24 NMS shall retrieve and process a service order, determine the assigned service, assigned DSLAM and ADSL port, and the physical link, the ATM port for the NSP (see the Service Order Management Section of this document).

PVC-NMS-25 NMS shall, for new-connects, determine the serving DSLAM, ADSL port and use the inventory of VPI/VCIs and assignment guidelines for the DSLAM Port and associated DSLAM-ATM interface, select and assign VPI/VCIs using a *to-be-defined* assignment algorithm (see PVC-NMS-12).

PVC-NMS-26 NMS shall determine if the elements in the selected or pre-defined path (ATM switches, DSLAMs, ADSL ports, switch ports, facilities) are valid. The user should be notified if errors are detected.

PVC-NMS-27 NMS shall provision the VCC across each subnetwork by communicating with the DSLAM using the TL/1 interface and with the Ascend NavisXtend Provisioning Server SNMP Interface.

PVC-NMS-28 NMS shall report completion and failures to the user. If failures are detected, return the network to its original state (i.e., undo any partial assignments). If no failures are detected, maintain records of successfully established end-to-end PVCs.

PVC-NMS-29 When a PVC is deleted, NMS shall delete the PVC across all network resources allocated to the network connection. All alerts associated with the PVC shall be cleared first.

Figure 7-6 illustrates this flow.

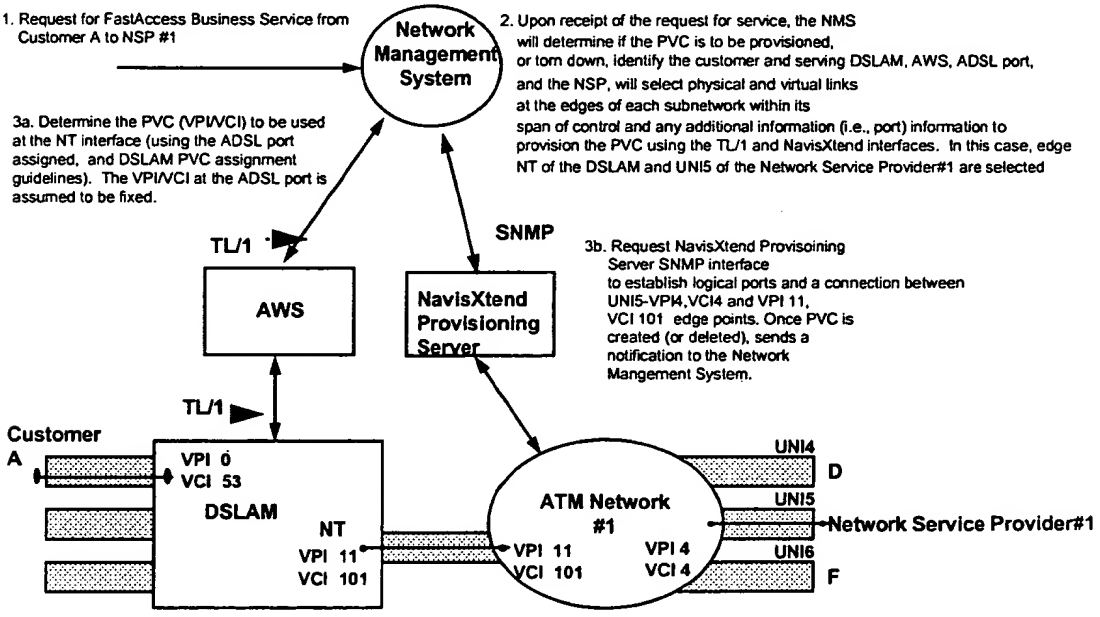

Figure 7-6. Logical Provisioning End-Customer to NSP

7.3.1.3 Provisioning Virtual Path Connection (DSLAM to Service Gateway)

The VPC between a DSLAM and a Service Gateway is provisioned across the ATM subnetwork from the ATM link termination port the DSLAM and a ATM link termination port of the Service Gateway.

PVC-NMS-30 NMS shall support a NMS User interface to create (or delete) a VPC from a DSLAM to a Service Gateway. The NMS User shall specify the

- The action (create or delete)
- The DSLAM and Service Gateway Identifiers
- The VPIs to be used at each end of the VPC.

PVC-NMS-31 NMS shall determine if the elements in the selected or pre-defined path (ATM DSLAM, ATM subnetwork port terminations, Service Gateway identifier) are known to NMS. The user shall be notified of any are unknown to NMS.

PVC-NMS-32 NMS shall provision or delete the VPC across the ATM Network using the NavisXtend Provisioning Server SNMP interface. The steps are identical to those for establishing a VCC, with the exception that the VCI should be set to zero (0) at the virtual path termination points (lport).

PVC-NMS-33 NMS shall report completion and failures to the user. If failures are detected, return the network to its original state (i.e., undo any partial assignments).
PVC-NMS-34 If no failures are detected, NMS shall for a new connect, create a PVC-ID and update its database with the VPC information including the VPI assignments at the edges of the VPC. For a deletion, the original PVC-ID and all references to the VPC shall be deleted.

PVC-NMS-35 When a PVC-ID is deleted, NMS shall delete the PVC across all network resources allocated to the network connection. All alerts associated with the PVC shall be cleared first.

7.3.1.4 Provisioning VCC from NSP to Service Gateway

The VCC between a NSP and a Service Gateway is provisioned across the ATM subnetwork from the ATM link termination port the NSP-ID and a ATM link termination port of the Service Gateway.

PVC-NMS-36 NMS shall support a NMS User interface to create (or delete) a VCC from a NSP-ID to a Service Gateway. The NMS User shall specify the

- The action (create or delete)
- The NSP and Service Gateway Identifiers
- The VPI/VCIs to be used at each end of the VCC (optional).

PVC-NMS-37 NMS shall determine if the elements in the selected or pre-defined path (NSP ID. ATM NSP and ATM subnetwork port terminations, Service Gateway identifier) are known to NMS. The user shall be notified of any are unknown to NMS.

PVC-NMS-38 NMS shall provision or delete the VCC across the ATM Network using the NavisXtend Provisioning Server SNMP interface. The steps are identical to those for establishing a VCC, described in establishing an ATM subnetwork connection for FastAccess service to a NSP.

PVC-NMS-39 NMS shall report completion and failures to the user. If failures are detected, return the network to its original state (i.e., undo any partial assignments).

PVC-NMS-40 If no failures are detected, NMS shall for a new connect, generate a PVC-ID and update its database with the VCC information including the VPI/VCI assignments at the edges of the VCC. For a deletion, the original PVC-ID and all references to the VCC shall be deleted.

PVC-NMS-41 When a PVC is deleted, NMS shall delete the PVC across all network resources allocated to the network connection. All alerts associated with the PVC shall be cleared first.

7.3.1.5 PVC Inventory Management

PVC inventory management addresses the following features:

PVC-NMS-42 NMS shall manage the inventory of PVCs (VCCs and VPCs) routed through the network, specifically from the subnetwork edge to subnetwork edge cross connect relationship. The inventory of these PVCs will support the fault management and testing functions, as well as provisioning functions associated the selection and assignment of PVCs. This high-level view is intended to prevent contention in the assignment of resources within the network.

This inventory can be created by retrieving ATM PVC assignments and cross connections within the network for each of the FastAccess assignable resources. This process is useful for initial inventory creation and on-going synchronization. The steps for the Alcatel DSLAMs are for each customer and assigned ADSL port in NMS, use the TL/1 commands *RTRV-VCL* and *RTRV-CRS-VC* to determine the VCCs. The PVC-ID will the Customer's TN-VPI-VCI at the ADSL port. To retrieve the ADSL profile information for the ADSL port, the RTRV-ADSL command shall be used.

7.3.1.6 Errors

PVC-NMS-43 NMS shall generate the following alerts to indicate errors encountered in provisioning or deleting PVCs.

Alert Name ***PVC-INTERFACE-NOT AVAILABLE***

Description:	DSLAM or ATM subnetwork interface not available or not responding {interface}
Affected Object:	Interface (i.e., gateway)
Severity:	Critical
Caused By:	The interface to is not active or the request has timed-out.
Cleared By:	Manual Clear
Causes and Actions:	Determine if the Gateway has been initialized. System administrator action required to determine the cause of the problem.

Alert Name ***PVC-EQUIPMENT-NOT AVAILABLE***

Description: NMS {port id}	ADSL ports, NT ports or ATM ports are unknown to
Affected Object:	DSLAM or ATM subnetwork
Severity:	Critical
Caused By:	The ports specified do not exist in NMS
Cleared By:	Manual Clear
Causes and Actions:	System administrator action required to determine the cause of the problem.

Alert Name ***PVC-DUPLICATE-PVC***

Description:	PVC already exists.
Affected Object:	PVC
Severity:	Critical
Caused By:	A request to create a VCC or VPC that already exists
Cleared By:	Manual Clear
Causes and Actions:	The request may have been processed previously. Use the NMS interface to retrieve the PVC. System administrator action required to determine the cause of the problem.

Alert Name ***PVC-UNKNOWN- PVC***

Description:	PVC does not exist in NMS
Affected Object:	Customer ID, NSP ID, DSLAM or ATM Subnetwork
Severity:	Critical
Caused By:	A request to delete a VCC or VPC that does not exist in NMS
Cleared By:	Manual Clear
Causes and Actions:	The request may have been processed previously. Use the NMS interface to retrieve the PVC. System administrator action required to determine the cause of the problem.

7.3.1.7 Questions/Issues

1. Parameters specific to Alcatel profiles and standard numbering schemes for these profiles need to be determined.
2. Parameters (i.e., attributes) to be set for the ATM subnetwork ATM logical connections need to be determined.

8. Fault Management Requirements

8.1 Purpose

The overall FastAccess fault management environment is described in the OTP [1]. This section focuses on the NMS fault management functions (see Figure 2-3). The NMS will receive all DSLAM TL1 alarms and all NavisXtend Fault Server alarms that pertain to the FastAccess network and service. The alarms gathered at the NMS will include all logical (i.e., ATM), physical (i.e., equipment, facilities), and (certain) subscriber-specific alarms. The NMS will also send a copy of the TL1 facility alarms to NMA for alarm correlation and presentation to NRC.

In Release 1, the Service Gateway alarms will be processed by the Service Gateway EMS, not NMS. In a subsequent release of NMS, the Service Gateway alarms will be forwarded to NMS.

FastAccess NMS features described in this section focus on alarm surveillance and include the following:

- Alarm surveillance: receiving alarms/events from
  - DSLAMs using a TL1 interface
  - ATM network using the Ascend Fault Server SNMP interface to report only a subset of the ATM Subnetwork that pertains to the FastAccess Services
  - Service Gateway (R2 feature)
- Alarm/event processing and correlation to determine the root-cause of a reported event across the FastAccess network and the affect on FastAccess customers and NSPs
- Alarm reporting and logging.

8.2 Dependencies

- Interfaces to Ascend's NavisXtend Fault Server and Alcatel's TL1 interface to DSLAMs and the Service Gateway (R2) are used for event reporting.
- Event, trap, and rule maps associated with Ascend's NavisXtend Fault Server are configured to forward only the FastAccess related alarms to NMS.

8.3 Assumptions

The assumptions used in the development of Fault Management requirements are as follows:

- Specific functions to support a FastAccess help desk are not addressed. The help desk may call the DCSC to determine the status of customer's service.

Alternatively, the help desk may have limited access to the NMS and functions described in this section.

- Each EMS will perform alarm correlation within the subnetwork (domain) that it monitors. Hence, the NMS will only perform cross-domain alarm correlation.
- NMS will analyze the received alarms to see if an alert should be generated (or cleared). All alarms sent to the NMS will ne logged.
- DCSC will monitor ATM subnetwork using NavisCore or the NavisXtend Fault Server and take appropriate corrective action (this includes all alarms that do not have an immediate impact on FastAccess service). The NMS will only monitor a subset of ATM subnetwork alarms related to the FastAccess service.
- NMS will only process NavisXtend Fault Server alarms which pertain to the FastAccess service. If a Fault Server alarm does not directly impact the FastAccess service, NMS should not receive it. This requires DCSC to configure the Fault Server to only forward the FastAccess alarms to NMS.
- In defining Ascend alarms to be forwarded to the FastAccess NMS (see Section 8.5.2), it is assumed that if a redundant card switch over takes place that only the associated, REDUND_CARD_SO alarm will be generated and that a CARD_DOWN alarm will not be generated for this card. Similarly, it is assumed that if a circuit reroute takes place the associated alarm CKT_REROUTE will be generated and the CKT_DOWN alarm will not be generated for this circuit.
- It is assumed that circuit alarm (CKT_DOWN, CKT_UP) detected by switches within the Ascend network will propagate to the switches at the edge of the network.
- The Ascend ATM alarms are sent to NMA independent of the FastAccess NMS. That is, the NMS will not forward any of the ATM SNMP traps to NMA.
- The TL1 alarms on facilities terminating on DSLAM (DS1, DS3, OC3) are forwarded to NMA by NMS.
- For the consumer services the ADSL port alarms are recommended to be "disabled" at the DSLAM. If needed, the NMS user can see these alarms through the AWS.
- For business services, the ADSL port alarms are recommended to be "enabled" at the DSLAM. Hence, these alarms will be received at the NMS.

8.4 Feature Description and Flow

The general approach to fault management is based on the vendor-specific element management system capabilities and reported alarms. A layered approach for monitoring events and isolating troubles will be used. This approach assumes that the EMSs for the ATM subnetwork, ADSL access and the Service Gateway (R2) will be used for element management layer fault monitoring and localization. The NMS will be used to monitor FastAccess physical and logical resources from a network and service perspective. Once the NMS has been notified of a specific alarm, the NMS user may need to access the appropriate EMS(s) for further trouble isolation.

8.4.1 NavisExtend Fault Server

Ascend's NavisXtend Fault Server is an intelligent agent that processes switch trap information via SNMP. A single Fault Server is expected to accommodate all Ascend switches used to support FastAccess services. The Fault Server will be used to buffer and process Network Element Layer (e.g., switch) traps before being sent to the NMS. This intermediate step offloads a significant amount of real-time NMS processing that could prove to become unwieldy in a large network.

The Fault Server receives SNMP traps generated by Ascend network elements. Ascend offers a wide variety of traps for alarm indications, threshold crossing and event notification regarding switches, trunks, physical ports, logical ports, and PVCs. The Fault Server provides a central repository and retrieval mechanism to obtain traps across an Ascend network based on specific filter criteria. The Fault Server does not control the generation of traps or the setting of alarm thresholds from the switch. It does, however, generate traps for alarm forwarding and trap forwarding.

Figure 8-1 illustrates the flow of traps through the Fault Server.

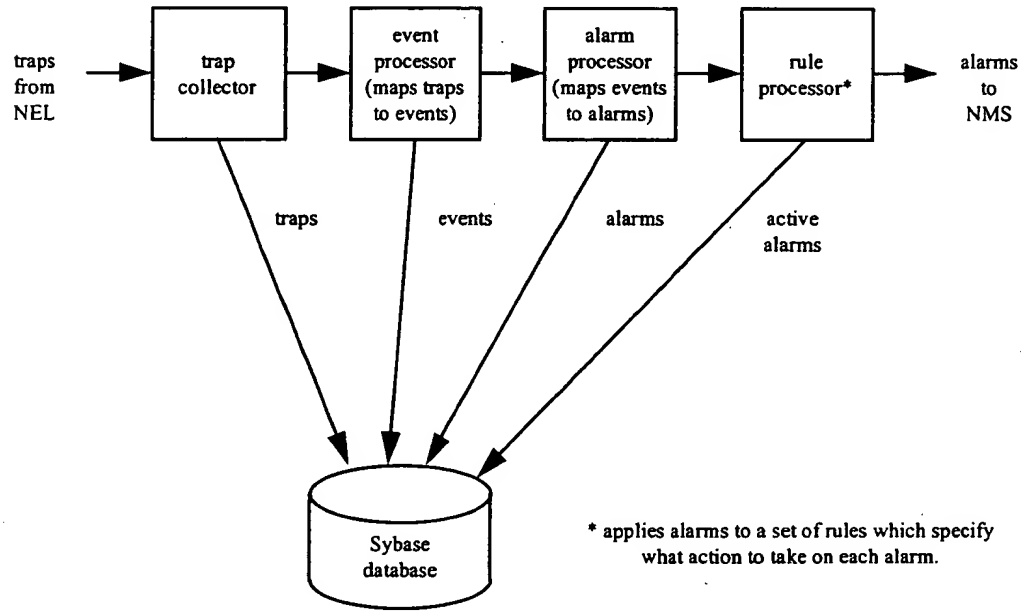

Figure 8-1. Trap Processing within Ascend's Fault Server

Storage

The Fault Server collects, processes, and stores traps in a Sybase database. NMS and DCSC diagnosticians may query this database to view specific fault information and obtain information related to each trap, including correlated alarm message, alarm aging, alarm severity, etc.

Processing
A set of filters (maps) are applied to all incoming traps. These filters determine how a trap traverses unique filtering in several stages from a trap to an event to an alarm.

The **trap collector** serves as a high-speed buffer of incoming switch traps. This is an important feature as numerous traps can result from a single network problem. The trap collector can also recover certain traps that may have become lost before reaching the Fault Server. The trap collector examines the sequence number of each trap to ensure that all have been received. Certain traps, referred to as reliable traps, are copied into a buffer from the switch where they originate. The trap collector can request for a switch to resend lost traps. The trap collector stores the trap source (switch), time, and other trap information in the Sybase database.

The **event processor** applies each trap to a set of event maps (filters) to determine if it should become an event. Each qualified event is stored in the Sybase database and forwarded to the alarm processor. More than one event can be generated from a single incoming trap.

The **alarm processor** applies each incoming event to a set of alarm maps to determine if they should become an alarm. Each qualified alarm is stored in the Sybase database and sent to the rule processor. The alarm processor supports single alarms and group alarms. Group alarms are groups of events that ultimately form a single alarm. Their purpose is to correlate multiple events and allow them to cause a single alarm condition. An intermittent physical port, for example, may repeatedly change states from up to down, and distinct events are created each time. The alarm processor can generate one alarm to indicate an "unsettled state" in such a scenario. More than one alarm can be generated from a single event.

The **rule processor**, the final component in the Fault Server, forwards qualified alarms to NMS using traps. It applies each alarm to a set of rules to determine what action to take on the alarm. If there are no rules applied to the alarm, the alarm is immediately sent to archive. If there are rules that apply to the alarm, the rules are invoked. The applied rules may cause the alarm to be closed, held, or subjected to some other such action. Once an alarm passes through the rules, the alarm then becomes active.

Alarm forwarding is performed by applying each alarm to a set of filters (maps) to determine if the alarm should be forwarded. Only an alarm that meets the criteria specified by a particular map is directed to the NMS.

See reference [4] for more details on the trap collector, event processor, alarm processor, and rule processor.

8.4.2 Alcatel Autonomous Messages

Each DSLAM supports the generation of autonomous messages to report alarms and events occurring within the DSLAM. An AWS supports a separate interface that consolidates the autonomous messages for all the DSLAMs that it manages. Autonomous messages are unsolicited and generated automatically as a result of events detected by the system. While there are four categories of event messages, only the autonomous alarm messages are processed for NMS fault management Release 1 requirements.

8.4.3 NMS Alarm Processing

Figure 8-2 illustrates the passing of alarms from the Alcatel DSLAMs (through the Alcatel EMS) and ATM (Ascend Switches [Network Elements or NEs] and Fault Server) domains to the NMS and the steps the NMS takes in processing the incoming alarms. The three steps taken by the NMS are outlined below. Specific details on correlation, processing, and alert generation can be found in Section 8.5.

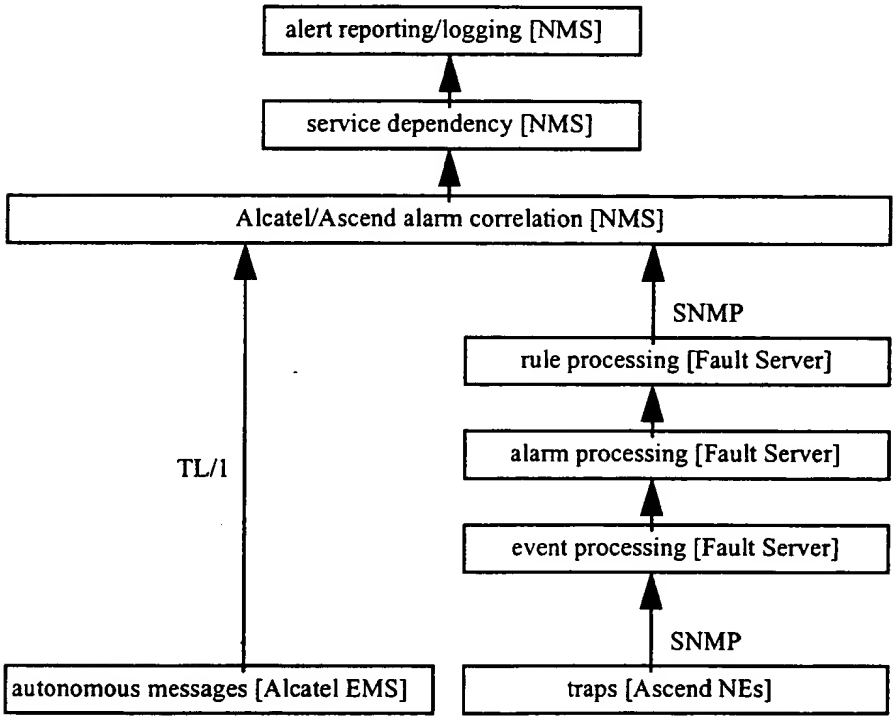

Figure 8-2. Alarm Flow

Alcatel/Ascend Alarm Correlation

Alarm correlation is needed when one network event causes alarms by both the ATM and ADSL domains. For example, in the case of physical link failures, both ends of the link will receive and generate notifications. Within the NMS, correlation associated with physical link failures will depend upon the end-points of the physical link (i.e., DSLAM, Service Gateway, or NSP). In the case of the end points being the DSLAM and the ATM network, the NMS processes all alarms from DSLAMs and alarms from NavisXtend Fault Server to determine if they are correlated. For example, a failure of a physical port at one end will cause alarms at the other end. In this case, the root cause is the port failure. In the case of a physical link failure between the DSLAM and ATM subnetwork, both the DSLAM and ATM port will detect failures. These failures will be correlated to determine if the root cause is the physical link failure. Once the root cause is determined, other alarms related to that event will be suppressed.

Service Dependency
NMS processes all received alarms to determine whether they affect FastAccess end-customers or NSP. The following associations must be supported by the NMS to process the alarms:

- DSLAM alarms can be directly associated with end-customers
- ATM alarms must be associated to either the physical link or virtual circuit supported to determine affected DSLAM, Service Gateway, or NSP.

Alarm Reporting and Logging
The NMS will generate its own alerts based on the correlation and service dependency determined. All incoming alarms from NavisXtend Fault Server and the DSLAMs will be logged.

Individual subscribers and NSP customers will be treated differently. Individual alerts of customers affected by an incoming event will not be generated. However, it is an objective that a log be created that can be updated with customer affecting events. It can then be determined if a customer is affected by entering in the Customer ID (TN) that may be used to pull up a history of events related to that customer sorted by date and time. These logs may then be used to generate reports to calculate such things as average down time per customer. For NSP customers, 'NSP Alerts' will be generated.

The NMS will also forward Alcatel DSLAM TL1 alarms to NMA. Figure 8-3 provides an example of a physical-layer alarm flow originating from the DSLAM to NMA.

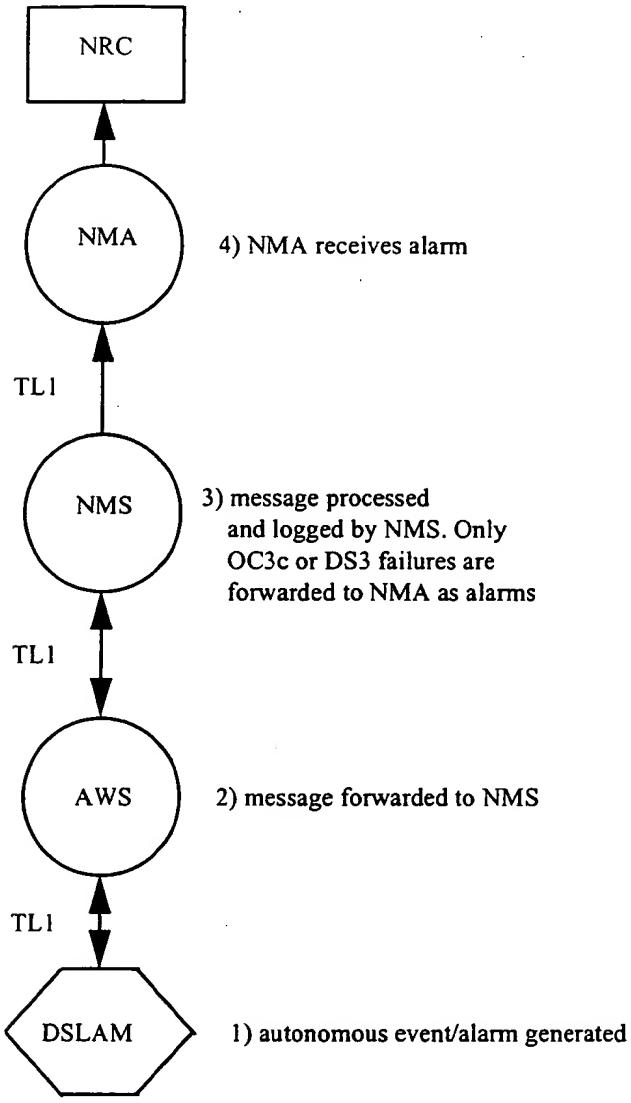

Figure 8-3. Example of Physical-Layer Alarm Flow Originating from DSLAM

8.5 Release 1 Requirements

8.5.1 General (R1)

FM-NMS-1 NMS shall display a network map of the states in the BellSouth region. This map shall be used to reflect the highest severity alert associated with the FastAccess equipment in a state. Only alerts generated by Fault Management shall be reflected on

this map (i.e., network creation, service order management, PVC management alerts shall not be reflected).

FM-NMS-2 NMS shall update the Network Map to reflect receipt and clearing of alerts using the following functions:

- Associate lower-level subnetwork components/locations to the appropriate higher level location/component (i.e., alerts are "bubbled up").
- The color of each state shall be based on the highest severity alarm associated with the subnetwork components located with in each state using standard color schemes: Critical- red, Major-orange, Minor-yellow, and no alarm - green.

FM-NMS-3 NMS shall allow the NMS user to select a state from the map to display a list of all LATAs containing FastAccess equipment. This list shall also reflect the highest severity alarm associated with the FastAccess equipment in a building location associated with a LATA.

FM-NMS-4 NMS shall allow the NMS user to select a building location to display a list of all the FastAccess equipment within that Location. This list shall reflect the highest severity alarm associated with the FastAccess equipment within the building location.

FM-NMS-5 NMS shall reflect the highest severity alarm associated with any NMS network equipment in response to any GUI to retrieve network configuration information.

FM-NMS-6 NMS shall log all NMS generated alerts for access by a notification screen (e.g., an alert window).

- The log entries shall contain the following:
  - Alert type
  - Alert description
  - Date and time of alarm
  - Alert severity
  - Affected network component
  - Probable cause
  - Alert status (acknowledged, cleared, etc.)
  - Recommended action to be taken.
- All active NMS alerts shall be retrievable for display on the GUI notification screen (alert window).
- Alert filters for a specific user alert window (for dividing network surveillance responsibilities) shall be supported. A minimum of three filters shall be supported: one for all network creation alarms, one for all service order processing alarms, and one for all network/service alarms.
- Multiple customized alarm windows shall be supported. The minimum is three: one for Service Order management alerts, one for NMS Network

Creation/DSLAM Capacity Management alerts, and one for NMS Fault Management alerts.

- An alert window shall be customizable to support audible alerts, number of events displayed and order of events displayed (i.e., by date, severity, equipment).
- The ability to protect selected alarms from being manually cleared from the alarm display window shall be supported (i.e., alarms associated with network creation).
- Alert windows shall be accessible remotely by authorized users.

FM-NMS-7 NMS shall allow an authorized NMS user to acknowledge an NMS alert on the alert window.

FM-NMS-8 NMS shall allow an authorized NMS user to clear an NMS alert on the alert window.

FM-NMS-9 NMS shall sort and filter (count redundant/persistent) NMS generated alerts by affected network component.

FM-NMS-10 NMS shall maintain a history log of all NMS generated alerts (and associated clears). Report generation tools shall be available to an authorized user to manipulate this history data to support trouble analysis. Examples of trouble analysis are:

1. Studies of network components that fail with some selected level of persistence
2. Ports and links that have had frequent indications of protocol errors or congestion
3. Network outage reports
4. Service outage reports
5. Daily summary of alarm frequencies.

FM-NMS-11 NMS shall maintain a log of all alarms received from the DSLAMs and NavisExtend Fault Server. These logs shall be backed up and then refreshed once a day. The daily logs shall be retained for 7 days.

FM-NMS-12(O) NMS shall support a log of end-customers affected by NMS generated alerts and NMS clearing of alerts. The following information should be logged for each customer affected by NMS Alert processing: Customer Name, TN, Date, Time, NMS Alert, NMS Alert action (Generate or Cleared), Alert severity, NMS affected object for the alert.

FM-NMS-13 The NMS shall forward a copy of the Alcatel TL1 autonomous message associated with facility alarms (i.e., RPT ALM OC3 and RPT ALM T3) to NMA.

8.5.2 Ascend Alarm Processing and Correlation Features (R1)

FM-NMS-14 NMS shall process the following alarms generated by the NavisExtend Fault Server[7]:

- CARD_UP - reports when card has become active on ATM switch
- CARD_DOWN - reports when card has become inactive on ATM switch
- PPORT_UP - reports when physical link failure has been cleared on an ATM switch port
- PPORT_DOWN - reports when physical link failure has been detected on ATM switch port
- CKT_UP - reports when an ATM virtual circuit has become active
- CKT_DOWN - reports when an ATM virtual circuit has become inactive

FM-NMS-15 The NMS shall receive the following SNMP trap for all alarms it receives from the Fault Server. This trap is generated by the Fault Server after incoming NE traps are processed by the event processor, alarm processor, and rules processor in the Fault Server.

```
fltsrvAlarmTrap TRAP-TYPE
    ENTERPRISE cascfltsrv
    VARIABLES { fltsrvSeverity, fltsrvComponentID, fltsrvAlarmText }
    DESCRIPTION
    "This trap is generated by the Fault Server when an alarm is
    opened or closed."
    ::= 130
```

The fltsrvAlarmTrap contains information on the alarm, components affected and severity level. The variables included in this trap are described below.

```
fltsrvSeverity OBJECT-TYPE
     SYNTAX  INTEGER {
        critical(1),
        major(2),
        minor(3),
        warning(4),
        info (5),
        cleared(6)
     }
     ACCESS  read-only
     STATUS  mandatory
```

[7] The NavisXtend Fault Server shall be configured to support the forwarding of these alarms on FastAccess ATM resources.

```
    DESCRIPTION
      "This is the severity that the alarm is being changed to."
    ::= { cascfltsrv 1 }

fltsrvComponentID OBJECT-TYPE
    SYNTAX  OCTET STRING
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "This is the component ID for the component that the alarm
       transition applies to. The format of this string is :
       <switch IP>-<card number>-<Pport>-<Channel>-<Lport>-<Circuit>

       This should enable the receiver to identify the specific
       object that is effected by this alarm."
    ::= { cascfltsrv 2 }

fltsrvAlarmText OBJECT-TYPE
    SYNTAX  OCTET STRING
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "This is a text string that describes the alarm condition.
       It is assumed that the severity field will identify whether
       an alarm condition is opened or closed. An example of a
       alarm text may be Logical Port Down. A severity value of
       normal would mean that this condition had been cleared."
    ::= { cascfltsrv 3 }
```

FM-NMS-16 The NMS shall identify the PPORT_DOWN trap and retrieve information contained in trap as follows.

The Fault Server generates a fltsrvAlarmTrap containing the following extractable information:

- Trap Binding 1 (fltsrvSeverity) = 2 (major)
- Trap Binding 2 (fltsrvComponentID) = <switch IP><card number><Pport>
- Trap Binding 3 (fltsrvAlarmText) = PPORT_DOWN.

FM-NMS-17 The NMS shall process the PPORT_DOWN alarm as follows.

For the physical link associated with the pport determine what is connected at the far end of the physical link using information contained in NMS database.

If far end of physical link = DSLAM
...identify NT card associated with DSLAM
...If there are no alerts against the DSLAM NT card or DSLAM, generate the FM-PHYSICAL-LINK alert and
...(OBJECTIVE: determine customers served by DSLAM using NMS database)
...(OBJECTIVE: write event to *Affected End-Customer Log* (FM-NMS-12)

If far end of physical link = NSP
...generate FM-PHYSICAL-LINK Alert
generate FM-NSP-ATM-PORT-DOWN Alert

If far end of physical link = SG
...generate *FM-PHSYICAL-LINK Alert*
...identify all virtual circuits supported on pport
...determine for each virtual circuit if end point at DSLAM or NSP
if DSLAM (OBJECTIVE: determine customer associated with virtual circuit)
(OBJECTIVE: write event to *Affected End-Customer Log* defined in FM-NMS-12)
if NSP, generate FM-NSP-ATM-PORT-DOWN Alert

If far end of physical link = Other
...do not generate any alerts

FM-NMS-18 The NMS shall identify the PPORT_UP trap and retrieve information contained in the trap as follows.

The Fault Server generates a fltsrvAlarmTrap containing the following extractable information:

- Trap Binding 1 (fltsrvSeverity) = 6 (cleared)
- Trap Binding 2 (fltsrvComponentID) = <switch IP><card number><Pport>
- Trap Binding 3 (fltsrvAlarmText) = PPORT_UP

FM-NMS-19 The NMS shall process the PPORT_UP alarm as follows.

For the physical link associated with the pport (determined from NMS database) determine what is connected at the far end of the physical link using information contained in NMS database.
Clear *FM-PHYSICAL-LINK Alert*

If far end of physical link = DSLAM
...(OBJECTIVE: determine customers served by DSLAM using NMS database)
...(OBJECTIVE: write event to *Affected End-Customer Log* defined in FM-NMS-12)

If far end of physical link = NSP
...clear *FM-NSP-ATM-PORT-DOWN Alert* previously generated

If far end of physical link = SG
...identify all virtual circuits supported on pport
...determine for each virtual circuit if end point at DSLAM or NSP
if NSP clear *FM-NSP-ATM-PORT-DOWN Alert* previously generated
if DSLAM (OBJECTIVE: determine customer associated with virtual circuit)
(OBJECTIVE: write event to *Affected End-Customer Log* defined in FM-NMS-12)

If far end of physical link = Other
...do not generate/clear any alerts

FM-NMS-20 The NMS shall identify the CARD_DOWN trap and retrieve information contained in the trap as follows.

The Fault Server generates a fltsrvAlarmTrap containing the following extractable information:

- Trap Binding 1 (fltsrvSeverity) = 1 (critical)
- Trap Binding 2 (fltsrvComponentID) = <switch IP><card number>
- Trap Binding 3 (fltsrvAlarmText) = CARD_DOWN

FM-NMS-21 The NMS shall process the CARD_DOWN alarm as follows.

For the each pport on a card (determined from NMS database) determine what is connected at the far end of the physical link of the pport using information contained in NMS database.

If far end of physical link = DSLAM
...generate *FM-ATM-CARD-DOWN Alert*
...identify NT card associated with DSLAM
...suppress any REPT ALM OC3 or REPT ALM T3 alarms generated by the associated NT card on the DSLAM and associated NMS FM-PHYSICAL-LINK alerts
...(OBJECTIVE: determine customers served by DSLAM using NMS database)
...(OBJECTIVE: write event to *Affected End-Customer Log* defined in FM-NMS-12)

If far end of physical link = NSP
...generate *FM-ATM-CARD-DOWN Alert*
...generate *FM-NSP-ATM-CARD-DOWN Alert*

If far end of physical link = SG
...generate *FM-ATM-CARD-DOWN Alert*
...identify all virtual circuits supported on pport
...determine for each virtual circuit if end point at DSLAM or NSP
if NSP generate *FM-NSP-ATM-CARD-DOWN Alert*
if DSLAM (OBJECTIVE: determine customer associated with virtual circuit)

(OBJECTIVE: write event to *Affected End-Customer Log* defined in FM-NMS-12)

If far end of physical link = Other
...do not generate any alerts

FM-NMS-22 The NMS shall identify the CARD_UP trap and retrieve information contained in trap as follows.

The Fault Server generates a fltsrvAlarmTrap containing the following extractable information:

- Trap Binding 1 (fltsrvSeverity) = 6 (cleared)
- Trap Binding 2 (fltsrvComponentID) = <switch IP><card number>
- Trap Binding 3 (fltsrvAlarmText) = CARD_UP.

FM-NMS-23 The NMS shall process the CARD_UP alarm as follows.

For the each pport on a card (determined from NMS database) determine what is connected at the far end of the physical link of the pport using information contained in NMS database.

If far end of physical link = DSLAM
...clear *FM-ATM-CARD-DOWN Alert* previously generated
...(OBJECTIVE: determine customers served by DSLAM using NMS database)
...(OBJECTIVE: write event to *Affected End-Customer Log* defined in FM-NMS-12)

If far end of physical link = NSP
...clear *FM-ATM-CARD-DOWN Alert* previously generated
...clear *FM-NSP-ATM-CARD-DOWN Alert* previously generated

If far end of physical link = SG
...clear *FM-ATM-CARD-DOWN Alert* previously generated
...identify all virtual circuits supported on pport
...determine for each virtual circuit if end point at DSLAM or NSP
if NSP clear *FM-NSP-ATM-CARD-DOWN Alert* previously generated
if DSLAM (OBJECTIVE: determine customer associated with virtual circuit)
(OBJECTIVE: write event to *Affected End-Customer Log* defined in FM-NMS-12)

If far end of physical link = Other
...do not generate/clear any alerts

FM-NMS-24 The NMS shall identify the CKT_DOWN trap and retrieve information contained in the trap as follows.

The Fault Server generates a fltsrvAlarmTrap containing the following extractable information:

8-14

- Trap Binding 1 (fltsrvSeverity) = 4 (warning)
- Trap Binding 2 (fltsrvComponentID) =

<switch IP><card number><Pport><Channel><Lport><Circuit>

- Trap Binding 3 (fltsrvAlarmText) = CKT_DOWN

FM-NMS-25 The NMS shall process the CKT_DOWN alarm as follows.

Determine what is connected at the far end of the circuit using information contained in NMS database.

If far end of virtual circuit = DSLAM
...generate *FM-ATM-CIRCUIT-DOWN Alert*
...(OBJECTIVE: determine customer associated with virtual circuit)
...(OBJECTIVE: write event to *Affected End-Customer Log* defined in FM-NMS-12)

If far end of virtual circuit = NSP
...generate *FM-ATM-CIRCUIT-DOWN Alert*
...generate *FM-NSP-ATM-CIRCUIT-DOWN Alert*

If far end of virtual circuit = Other
...do not generate any alerts

FM-NMS-26 The NMS shall identify the CKT_UP trap and retrieve information contained in the trap as follows.

The Fault Server generates a fltsrvAlarmTrap containing the following extractable information:

- Trap Binding 1 (fltsrvSeverity) = 6 (cleared)
- Trap Binding 2 (fltsrvComponentID) =

<switch IP><card number><Pport><Channel><Lport><Circuit>

- Trap Binding 3 (fltsrvAlarmText) = CKT_UP

FM-NMS-27 The NMS shall process the CKT_UP alarm as follows.

Determine what is connected at the far end of the circuit using information contained in NMS database.

If far end of virtual circuit = DSLAM
...clear *FM-ATM-CIRCUIT-DOWN Alert* previously generated
...(OBJECTIVE: determine customer associated with virtual circuit)
...(OBJECTIVE: write event to *Affected End-Customer Log* defined in FM-NMS-12)

If far end of virtual circuit = NSP

...clear *FM-ATM-CIRCUIT-DOWN Alert* previously generated
...clear *FM-NSP-ATM-CIRCUIT-DOWN Alert* previously generated

If far end of virtual circuit = Other
...do not generate/clear any alerts

8.5.3 Alcatel TL1 Alarm Message Processing and Correlation (R1)

FM-NMS-28 The NMS shall process the following TL/1 autonomous messages from the Alcatel DSLAMs (as received across the autonomous message interface):

- REPT ALM ADSL - reports current alarms associated with ADSL facilities in the DSLAM (i.e., the ADSL port and physical link to the ATU-R)
- REPT ALM ENV - reports environmental alarms from the DSLAM
- REPT ALM EQPT - reports current DSLAM equipment alarms
- REPT ALM OC3 - reports current OC3 facility alarms from the DSLAM (i.e., the physical link OC3 interface that may exist between the DSLAM and the ATM subnetwork)
- REPT ALM T3 - reports current T3 (DS3) facility alarms from the DSLAM (i.e., the physical link DS3 interface that may exist between the DSLAM and the ATM subnetwork).

FM-NMS-29 NMS shall parse and identify each of these messages as documented in the *"R2.3 TL1 Commands Interface Specification"* [2] and described below.

The message syntax is as follows:

<cr><lf><lf>
^^^sid yy-mm-dd hh:mm:ss<cr><lf>
<almcde>^<<atag>^VERB[^MODIFIER][^MODIFIER]<cr><lf>
^^^"<Message Detail>"<cr><lf>
;

Where

<cr>	Denotes a carriage return
<lf>	Denotes a line feed
^	Denotes a space
sid	The 11 character CLLI code of the DSLAM
yy-dd-mm	The date the message was generated
hh:mm:ss	The time that the message was generated
almcde	The severity of the message *C - Critical ** - Major *^ - Minor A^ - Automatic Message (used to report a cleared alarm)

atag	The autonomously generated correlation number generated automatically and sequentially by the DSLAM. Each message from a DSLAM will have a unique number.
VERB...	The message name.
"Message Detail"	Unique information pertaining to the alarm

FM-NMS-30 The NMS shall identify and parse the REPT ALM ENV as follows:

1. The first line of the autonomous message contains the *sid,* which is to be used as the DSLAM ID, a date and time stamp.
2. The subsequent line shall contain the alarm code *(almcde),* which identifies the severity of the message (*C, **, *^, A^), a sequential message number, and the message name REPT ALM ADSL. The alarm code is used by NMS to determine if an NMS alert should be generated or cleared.
3. The next line will contain the Message Detail, a string contained in " ", with each of the following fields separated by a comma. The Message Detail shall be parsed as follows (key fields for NMS processing are italicized) :
   - *aid-env* - the Environment AID
   - ntfncde - notification code associated with the condition (CR, MJ, MN, CL)
   - *cond-env* - the related environment condition (MISC)
   - ocrdat - Date of occurrence in mm-dd format
   - ocrtm - Time of occurrence in hh-mm format
   - *conddescr* = the description of the alarm (1-40 characters) as indicated under cond-adsl above.

FM-NMS-31 The NMS shall process the REPT ALM ENV as follows:

1. NMS shall determine if the DSLAM exists in the NMS. If it does not, the NMS alert, NC-UNKNOWN-DSLAM shall be generated. The alert description shall contain the DSLAM name, the *almcde* and *conddescr* and processing of this message will be completed.
2. If the DSLAM exists in NMS, NMS shall use the contents of the *almcde* field to determine if a NMS alert should be generated or cleared. If the *almcde* is "A", then the alert, FM-DSLAM-ENV shall be cleared for the DSLAM.
3. If the *almcde* field is not "A", then the alert FM-DSLAM-ENV should be generated for the DSLAM.

FM-NMS-32 The NMS shall identify and parse the REPT ALM ADSL as follows:

1. The first line of the autonomous message shall contain a valid DSLAM CLLI code *(sid)*, date and time stamp.
2. The subsequent line shall contain the alarm code *(almcde),* which identifies the severity of the message (*C, **, *^, A^), a sequential message number, and the message name REPT ALM ADSL. The alarm code is used by NMS to determine if an NMS alert should be generated or cleared.

3. The next line will contain the Message Detail, a string contained in " ", with each of the following fields separated by a comma. The Message Detail shall be parsed as follows (key fields for NMS processing are italicized):
   - *aid-adsl* - the access identifier in the form of ADSL-rack-shelf-lt_slot-circuit (where rack = 1..4, shelf = 1..4, lt_slot = 1-12, circuit = 1-4)
   - ntfncde - notification code associated with the condition (CR, MJ, MN, CL)
   - *cond-adsl* - the related line condition
     - LOS - Loss of signal; not service affecting; minor
     - FACTERM - Modem was unable to initialize; service affecting; major
     - LCD-I - Loss of cell delineation - interleaved; service affecting; minor. This is designed for video services and shall be ignored by NMS.
     - LCD-F - Loss of cell delineation - fast; service affecting; minor.
   - *serveff* - SA = Service Affecting, immediate action required; NSA = not service affecting
   - ocrdat - Date of occurrence in mm-dd format
   - ocrtm - Time of occurrence in hh-mm format
   - *locn* - NEND = near end, FEND = Far end
   - *dirn* - the direction of the received condition (RCV= receive, TRMT= transmit)
   - *conddescr* = the description of the alarm (1-40 characters) as indicated under cond-adsl above.

FM-NMS-33 The NMS shall process the REPT ALM ADSL as follows:

1. The internal NMS name for the ADSL port shall be formed by concatenating the *sid* field (the DSLAM CLLI code) to the rack-shelf-lt_slot-circuit in the *aid_adsl* field.
2. NMS shall determine if the ADSL port exists in the NMS.
   If it does not, the NMS alert, NC-UNKNOWN-PORT, shall be generated. The alert description shall contain the ADSL port name, the *almcde* and *conddescr*. Processing this message will be completed.
3. If the ADSL port exists in NMS, NMS shall use the contents of the *almcde* field to determine if a NMS alert should be generated or cleared. If the *almcde* is "A," then the alert should be cleared. The contents of the *cond_adsl* field are used to determine the associated NMS alert.
4. NMS shall determine all the customers served by the ADSL port and write an entry in the Affected End-Customer Log reflecting the generation of the alert or the clearing of the alert.
5. Based on the contents of the *cond_adsl* field, the following alarms should be generated (or cleared) for the ADSL port:

ADSL Condition	NMS Alert	Generate NMS Alert	Alert Description Information
LOS	FM-ADSL-PORT -LOS	If port is assigned to business service OR if port is assigned to consumer service and *locn* is NEND and *dirn* is TRMT	*cond-adsl, locn, dirn, customerID*
FACTERM	FM-ADSL-PORT-FACTERM	Always	*cond-adsl, locn, dirn, customerID*
LCD-F	FM-ADSL-PORT-LCD	Always	*cond-adsl, locn, dirn, customerID*

FM-NMS-34 The NMS shall identify and parse the REPT ALM EQPT as follows:

1. The first line of the autonomous message contains a DSLAM ID code (*sid)*, date and time stamp.
2. The subsequent line shall contain the alarm code (*almcde),* which identifies the severity of the message (*C, **, *^, A^), a sequential message number, and the message name REPT ALM EQPT. The alarm code is used by NMS to determine if an NMS alert should be generated or cleared.
3. The next line will contain the Message Detail, a string contained in " ", with each of the following fields separated by a comma. The Message Detail shall be parsed as follows (key fields for NMS processing are italicized):
   - *aid-eqpts* - the following equipment identifiers may be used:
     - NTA
     - RACK-rack
     - SHELF-rack-shelf
     - {ACUIEXIEXA}-rack-shelf (to describe the Alarm Control Unit or Shelf Extender Unit -A
     - LT-rack-shelf-lt_slot-circuit
   - ntfncde - notification code associated with the condition (CR, MJ, MN, CL)
   - *cond-eqpt* - the related equipment condition
     - EQPT - Equipment failed self test, major
     - MEMDIF - Plug-in module and configuration mismatch, minor, NSA
     - UNPLANNED - Module inserted in slot planned for NO-BOARD, minor, NSA
     - IM-PROPRMVL - improper removal of provisioned module, major
     - PROGVER - Failed to load or find requested software, major, NSA
     - RMTDLFAIL - Failed to download software, major, NSA
     - COMMERR - Failed to communicate with the module, Major
     - HITEMP - Module temperature exceeded limit, Major
     - CONTBUS - Subrack backplane Fault, Critical

  - BUSCFG - Backplane Configuration Error, Critical
  - CONTCOM - Subrack Extender Bus Fault, Critical
  - CONFIG - Invalid parameters in configuration, Minor
  - FA - fuse alarm. Power fuse blown, Minor
  - FANALM-1 - Fan alarm for Fan 1, Minor, NSA
  - FANALM-2 - Fan alarm for FAN-2, Minor, NSA
  - INIT - System and backup memory reset, Critical
  - SHUTDOWN - Equipment shut-down due to high temperature, Major
  - SWROLLBK - SW version rolled back, Minor, NSA
  - ATMHW - ATM hardware error, Major
  - IQCLKOOL - IQ-Bus clock not locked to reference, Critical
  - IQREFCLK - IQ-BUS reference clock lost, Critical.
- *serveff* - SA = Service Affecting, immediate action required; NSA = not service affecting
- ocrdat - Date of occurrence in mm-dd format
- ocrtm - Time of occurrence in hh-mm format
- *conddescr* = the description of the alarm (1-40 characters) as indicated under cond-eqpt above.

FM-NMS-35 NMS shall process the REPT ALM EQPT as follows:

1. NMS shall determine if the DSLAM exists in the NMS by using the SID as the DSLAM name. If it does not, the NMS alert, NC-UNKNOWN-DSLAM shall be generated. The alert description shall contain the DSLAM CLLI code, the *almcde* and *conddescr* and processing of this message will be completed.
2. If the DSLAM exists in NMS, the serveff field shall be used to determine if an alert shall be generated or cleared. If the serveff field is NSA, no alert shall be generated or cleared.
3. NMS shall use the contents of the *almcde* field to determine if a NMS alert should be generated or cleared. If the *almcde* is "A", then the alert should be cleared.
4. The contents of the *aid_eqpts* field shall be used to determine the associated NMS object as follows:
   - NTA shall reflect the NT port on the DSLAM (stored as DSLAM CLLI-NT in the NMS)
   - RACK-Rack shall be decoded to determine all associated ADSL ports
   - SHELF-rack-shelf shall be decoded to determine all associated ADSL ports
   - ACUIEXIEXA-rack-shelf shall be generated against the DSLAM
   - LT-rack-shelf-lt_slot-circuit shall be used to determine the ADSL ports.
5. Based on the contents of the *cond_eqpt* and *aid_eqpts* fields the following alarms should be generated (or cleared):

Equip	NMS Alert	Generate NMS Alert	Alert

Condition *cond_eqpt*			Description Information
EQPT	FM-ADSL-EQPT Write to Affected End-Customer Log	Against the DSLAM For all customers associated with the failed equipment.	*sid,* *cond_eqpt,* *aid_eqpts,* *conddescr*
IM- PROPRMVL	FM-ADSL-EQPT Write to Affected End-Customer Log	Against the DSLAM For all customers associated with the failed equipment	*sid,* *cond_eqpt,* *aid_eqpts,* *conddescr*
COMMERR	FM-ADSL-EQPT Write to Affected End-Customer Log	Against the DSLAM For all customers associated with the failed equipment	*sid,* *cond_eqpt,* *aid_eqpts,* *conddescr*
CONTBUS	FM-ADSL-EQPT Write to Affected End-Customer Log	Against the DSLAM For all customers associated with the failed equipment	*sid,* *cond_eqpt,* *aid_eqpts,* *conddescr*
HITEMP	FM-ADSL-EQPT Write to Affected End-Customer Log	Against the DSLAM For all customers associated with the failed equipment	*sid,* *cond_eqpt,* *aid_eqpts,* *conddescr*
BUSCFG	FM-ADSL-EQPT Write to Affected End-Customer Log	Against the DSLAM (*sid)* For all customers associated with the failed equipment	*sid,* *cond_eqpt,* *aid_eqpts,* *conddescr*
CONTCOM	FM-ADSL-EQPT Write to Affected End-Customer Log	Against the DSLAM (*sid*) For all customers associated with the failed equipment	*sid,* *cond_eqpt,* *aid_eqpts,* *conddescr*
INIT	FM-ADSL-EQPT Write to Affected End-Customer Log	Against the DSLAM (*sid*) For all customers associated with the failed equipment	*sid,* *cond_eqpt,* *aid_eqpts,* *conddescr*
ATMHW	FM-ADSL-EQPT Write to Affected End-Customer Log	Against the DSLAM (*sid*) For all customers associated with the failed equipment	*sid,* *cond_eqpt,* *aid_eqpts,* *conddescr*
IQCLKOOL	FM-ADSL-EQPT Write to Affected End-Customer Log	Against the DSLAM (*sid*) For all customers associated with the failed equipment	*sid,* *cond_eqpt,* *aid_eqpts,* *conddescr*
IQCLREFCLK	FM-ADSL-EQPT	Against the DSLAM (*sid*)	*sid,*

	Write to Affected End-Customer Log	For all customers associated with the failed equipment	*cond_eqpt, aid_eqpts, conddescr*
SHUTDOWN	FM-ADSL-EQPT Write to Affected End-Customer Log	Against the DSLAM (*sid*) For all customers associated with the failed equipment	*sid, cond_eqpt, aid_eqpts, conddescr*

FM-NMS-36 NMS shall identify and parse the REPT ALM OC3 as follows:

1. The NMS shall save all the lines associated with this autonomous message as received from the first <cr><lf><lf> to the message detail <cr><lf>, to forward onto NMA.
2. The first line of the autonomous message contains the DSLAM ID code (*sid)*, date and time stamp.
3. The subsequent line shall contain the alarm code (*almcde)* which identifies the severity of the message (*C, **, *^, A^), a sequential message number, and the message name REPT ALM OC3. The alarm code is used by NMS to determine if an NMS alert should be generated or cleared.
4. The next line will contain the Message Detail, a string contained in " ", with each of the following fields separated by a comma. The Message Detail shall be parsed as follows (key fields for NMS processing are italicized):
   - *aid_OC3* - OC3A is encoded
   - ntfncde - notification code associated with the condition (CR, MJ, MN, CL)
   - *cond_OC3* - the related line condition
     - AIS-L - Line Alarm Indication Signal, service affecting, minor
     - BERL-HT - Excessive Line Bit Errors, service affecting, critical
     - RFI-L - Remote failure/defect indication, service affecting, minor
     - T-CV-LFE - Excessive Far-End Block Errors, not service affecting, minor
     - T-CV-S - Excessive BIP-8 errors, not service affecting, critical
     - OOF- Section Out-Of-Frame, service affecting, critical
     - LOF - Section Loss-Of-Frame, service affecting, critical
     - LOS - Loss of signal; service affecting; critical
     - LOC - Loss of clock, service affecting, critical
     - CELLSIG - False start-of-cell input signal, service affecting, critical
     - OVRFLO - Buffer (FIFO) overflow, service affecting, critical
     - REFCLK - Reference clock failed, service affecting, critical
     - FIFOCLK - FIFO Clock failed, service affecting, critical
     - LCD - Loss of ATM Cell Delineation, service affecting, critical.
   - *serveff* - SA = Service Affecting, immediate action required; NSA = not service affecting
   - ocrdat - Date of occurrence in mm-dd format
   - ocrtm - Time of occurrence in hh-mm format
   - *locn* - NEND = near end, FEND = Far end

- *dirn* - the direction of the received condition (RCV= receive, TRMT= transmit)
- *conddescr* = the description of the alarm (1-40 characters) as indicated under cond_OC3 above.

FM-NMS-37 NMS shall process the REPT ALM OC3 as follows:

1. All entire REPT ALM OC3 autonomous message shall be sent onto NMA, as received by NMS (five lines):
   <cr><lf><lf>
   ^^^sid yy-mm-dd hh:mm:ss<cr><lf>
   <almcde>^<atag>^REPT ALM OC3 <cr><lf>
   ^^^"message detail" <cr><lf>
   ;
2. NMS shall determine the physical link associated with the DSLAM NT port termination for these alarms.
3. NMS shall determine the card terminating the physical link on the ATM switch.
4. NMS shall use the contents of the *almcde* field to determine if a NMS alert should be generated or cleared If the *almcde* is "A," then the alert should be cleared. The contents of the *cond_oc3* field to determine the associated NMS alert.
5. If an FM-ATM-CARD-DOWN alert does not exist on the ATM subnetwork end of the Physical Link, then based on contents of the *cond_oc3* field, the following alarms should be generated (or cleared) for the NT port:

OC3 Condition	NMS Alert	Generate NMS Alert	Alert Description Information
AIS-L	FM-NT-AIS-L	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_oc3, locn, dirn, conddescr*
BERL-HT	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_oc3, locn, dirn, conddescr*
RFI-L	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_oc3, locn, dirn, conddescr*
T-CV-S	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-	*cond_oc3, locn, dirn, conddescr*

		subnetwork termination of the physical link	
LOF	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_oc3, locn, dirn, conddescr*
LOS	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_oc3, locn, dirn, conddescr*
LOC	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_oc3, locn, dirn, conddescr*
CELLSIG	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_oc3, locn, dirn, conddesc*
OVRFLO	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_oc3, locn, dirn, conddescr*
REFCLK	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_oc3, locn, dirn, conddescr*
FIFOCLK	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_oc3, locn, dirn, conddescr*
LCD	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_oc3, locn, dirn, conddescr*

FM-NMS-38(O) For all the identified REPT ALM OC3 conditions that are major or critical, for which an NMS alert is being generated or cleared, NMS shall determine all the customers served by the DSLAM and for each, write an entry in the Affected End-Customer Log reflecting the generation of the alert or the clearing of the alert.

FM-NMS-39 NMS shall identify and parse the REPT ALM T3 as follows:

1. The NMS shall save all the lines associated with this autonomous message as received from the first <cr><lf><lf> to the message detail <cr><lf>, to forward onto NMA.
2. The first line of the autonomous message shall contain a valid DSLAM CLLI code (*sid*), date and time stamp.
3. The subsequent line shall contain the alarm code (*almcde*) which identifies the severity of the message (*C, **, *^, A^), a sequential message number, and the message name REPT ALM OC3. The alarm code is used by NMS to determine if an NMS alert should be generated or cleared.
4. The next line will contain the Message Detail, a string contained in " ", with each of the following fields separated by a comma. The Message Detail shall be parsed as follows (key fields for NMS processing are italicized):
   - *aid_ds3* - DS3NTA is encoded.
   - ntfncde - notification code associated with the condition (CR, MJ, MN, CL)
   - *cond_ds3* - the related line condition
     - RAI - Remote Alarm Indicator, service affecting, minor
     - AIS - Alarm Indication Signal, service affecting, minor
     - LOF - Loss-Of-Frame, service affecting, major
     - LOS - Loss of signal; not service affecting; critical
     - ATMFE - ATM DS3 PLCP Far-End Alarm, service affecting, major
     - ATMLOF - ATM DS3 PLCP Loss of Frame, service affecting, major
     - LCD - Loss of ATM Cell Delineation, service affecting, critical.
   - *serveff* - SA = Service Affecting, immediate action required; NSA = not service affecting
   - ocrdat - Date of occurrence in mm-dd format
   - ocrtm - Time of occurrence in hh-mm format
   - *locn* - NEND = near end, FEND = Far end
   - *dirn* - the direction of the received condition (RCV= receive, TRMT= transmit)
   - *conddescr* = the description of the alarm (1-40 characters) as indicated under cond-T3 above.

FM-NMS-40 NMS shall process the REPT ALM T3 as follows:

1. All entire REPT ALM T3 autonomous message shall be sent onto NMA, as received by NMS (five lines):

   <cr><lf><lf>
   ^^^sid yy-mm-dd hh:mm:ss<cr><lf>
   <almcde>^<atag>^REPT ALM T3 <cr><lf>
   ^^^"message detail" <cr><lf>
   ;

2. The internal NMS name for the DSLAM T3 port shall be formed by concatenating the *sid* field (the DSLAM CLLI) to "-NT".

3. NMS shall use the contents of the *almcde* field to determine if a NMS alert should be generated or cleared If the *almcde* is "A", then the alert should be cleared. The contents of the *cond_ds3* field to determine the associated NMS alert.
4. Based on contents of the *cond_ds3* field, the following alarms should be generated (or cleared) for the NT port:

T3 Condition	NMS Alert	Generate NMS Alert	Alert Description Information
RAI	FM-NT-RAI	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_ds3, locn, dirn, conddescr*
AIS	FM-NT-AIS	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_ds3, locn, dirn, conddescr*
LOF	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_ds3, locn, dirn, conddescr*
LOS	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_ds3, locn, dirn, conddescr*
ATMFE	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_ds3, locn, dirn, conddescr*
ATMLOF	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_ds3, locn, dirn, conddescr*
LCD	FM-PHYSICAL-LINK	If FM-ATM-CARD-DOWN alert doesn't exist on the ATM-subnetwork termination of the physical link	*cond_ds3, locn, dirn, conddescr*

FM-NMS-41(O) For all the identified REPT ALM T3 conditions that are major or critical, for which an NMS alert is being generated or cleared, NMS shall determine all the customers served by the DSLAM and for each, write an entry in the Affected End-Customer Log reflecting the generation of the alert or the clearing of the alert.

8.5.4 NMS Alerts

Alert Name ***FM-PHYSICAL-LINK***

Description:	A pport on an ATM switch has reported physical link failures. DSLAM affected = DSLAM ID, NSP affected = NSP ID.
Affected Object:	Physical Link
Severity:	Major (2)
Caused By:	Physical port reporting physical link failures (LOS, LOF, AIS, etc).
Cleared By:	Pport Up Alert or Manual Clear
Causes and Actions:	All customers supported by port are affected. To determine specific reason for PPORT_DOWN alarm see pportlinkdownreason in Ascend Fault Server log.

Alert Name ***FM-ATM-CARD-DOWN***

Description:	Card on defined ATM switch has gone down. DSLAM affected = DSLAM ID, NSP affected = NSP ID.
Affected Object:	Switch ID/Card ID
Severity:	Critical (1)
Caused By:	Card going down.
Cleared By:	Card Up Alert or Manual Clear
Causes and Actions:	All customers supported by card are affected

Alert Name ***FM-ATM-CIRCUIT-DOWN***

Description:	Virtual circuit has gone down.
Affected Object:	Switch ID/Card ID/Pport ID/Circuit ID
Severity:	Warning (4)
Caused By:	Circuit going down.
Cleared By:	Circuit Up Alert or Manual Clear
Causes and Actions:	All customers supported on circuit are affected. To determine specific reason for CKT_DOWN alarm see CktFailReason in Ascend Fault Server log.

Alert Name ***FM-NSP-ATM-PORT-DOWN***

Description:	Service to NSP is down.
Affected Object:	NSP ID
Severity:	Major (2)
Caused By:	Physical port going down. Provide Switch ID/Card ID/Pport ID.
Cleared By:	Pport Up Alert or Manual Clear
Causes and Actions:	All customers supported by port are affected.

Alert Name FM-NSP-ATM-CARD-DOWN

Description:	Service to NSP is down.
Affected Object:	NSP ID
Severity:	Major (2)
Caused By:	Card going down. Provide Switch ID/Card ID.
Cleared By:	Card Up Alert or Manual Clear
Causes and Actions:	All customers supported by card are affected.

Alert Name FM-NSP-ATM-CIRCUIT-DOWN

Description:	Virtual circuit to NSP is down.
Affected Object:	NSP ID
Severity:	Warning (4)
Caused By:	Virtual circuit going down. Provide Switch ID/Card ID/Pport ID/Circuit ID
Cleared By:	Circuit Up Alert or Manual Clear
Causes and Actions:	All customers on circuit are affected.

Alert Name FM-DSLAM-ENV

Description:	DSLAM Environmental Alarm
Affected Object:	DSLAM
Severity:	Minor
Caused By:	Autonomous message from DSLAM.
Cleared By:	Manual or via an automatic message from the DSLAM.
Causes and Actions:	Minor alarm and may have no impact on the service.

Alert Name FM-ADSL-PORT-LOS

Description:	Loss of Signal {location} {direction}
Affected Object:	ADSL Port
Severity:	Minor
Caused By:	Autonomous message from DSLAM. Loss of signal detected and the ADSL port supports business customer OR loss of signal detected, the port supports residential service, the location is near end and the direction is transmit.
Cleared By:	Manual or automatic message
Causes and Actions:	This indicates that the business customer has turned off their equipment or that there is a problem sending information to a residential customer.

Alert Name FM-ADSL-PORT-FACTERM

Description:	Modem was unable to initialize {location} {direction}
Affected Object:	ADSL Port
Severity:	Major
Caused By:	Autonomous message from DSLAM.
Cleared By:	Manual or automatic message
Causes and Actions:	This indicates that the modem is not working.

Alert Name FM-ADSL-PORT-LCD-F

Description:	Loss of cell delineation {location} {direction}
Affected Object:	ADSL Port
Severity:	Minor
Caused By:	Autonomous message from DSLAM.
Cleared By:	Manual or automatic message
Causes and Actions:	ATM processing errors.

Alert Name FM-ADSL-EQPT

Description:	{cond-eqpt} {aid_eqpt}
Affected Object:	DSLAM
Severity:	Major
Caused By:	Autonomous message from DSLAM.

Cleared By:	Manual or automatic message
Causes and Actions:	Customers may be affected.

Alert Name FM-NT-AIS-L

Description:	OC3 Line Alarm Indication Signal {equipment reported} {location} {direction}
Affected Object:	DSLAM NT Port
Severity:	Minor
Caused By:	Autonomous message from DSLAM.
Cleared By:	Manual or automatic message
Causes and Actions:	Customers may be affected.

Alert Name FM-NT-RAI

Description:	DS3 Remote Alarm Signal {equipment reported} {location} {direction}
Affected Object:	DSLAM NT Port
Severity:	Minor
Caused By:	Autonomous message from DSLAM.
Cleared By:	Manual or automatic message
Causes and Actions:	Customers may be affected.

Alert Name FM-NT-AIS

Description:	DS3 Alarm Indication Signal {equipment reported} {location} {direction}
Affected Object:	DSLAM NT Port
Severity:	Minor
Caused By:	Autonomous message from DSLAM.
Cleared By:	Manual or automatic message
Causes and Actions:	Customers may be affected.

Alert Name NC_UNKNOWN_DSLAM

Description:	DSLAM Autonomous message reported from a DSLAM unknown to NMS {sid}
Affected Object:	Tl/1 Autonomous message interface
Severity:	Major
Caused By:	Autonomous message from DSLAM.
Cleared By:	Manual or automatic message
Causes and Actions:	The TL/1 interface has reported a message for a DSLAM that does not exist in the NMS. Determine if the DSLAM name is incorrect in the NMS or if it should be added to the NMS.

Alert Name ***NC-UNKNOWN-ADSL-PORT***

Description:	DSLAM Autonomous message reported from a DSLAM ADSL port unknown to NMS {sid} {asl_aid}
Affected Object:	DSLAM
Severity:	Major
Caused By:	Autonomous message from DSLAM (REPT-ALM ADSL).
Cleared By:	Manual or automatic message
Causes and Actions:	The TL/1 interface has reported a message for a DSLAM ADSL port that does not exist in the NMS. Determine if the DSLAM ADSL port name is incorrect in the NMS or if it should be added to the NMS.

8.6 Release 2 Requirements

8.6.1 Alarm Reporting and Logging Features (R2)

FM-NMS- The NMS shall support an interface to allow an NSP to access to fault management information pertaining to NSP UNIs and possibly customers is to-be-defined. Several alternatives for providing access to this information are possible and include:

- Providing access to NMS and supporting a customized NSP alarm window,
- Use an SNMP interface to notify the NSP of faults
- Use a WEB based interface to notify the NSP of faults.

8.7 Issues

- The Alcatel TL/1 interface supports autonomous reporting of physical and environmental alarms only.
- Naming conventions for FastAccess assignable resources will need to be consistent with the information in the reported alarms.
- Service Gateway capabilities and interfaces supported are undefined.

9. Performance Management Requirements

9.1 Purpose of this Feature

Performance Management consists of a set of features to evaluate the effectiveness of the PC/DNA network and services. Performance Management involves the following:

- Garnering statistical data (from the ASAMs, DANAs and Ascend cbx500 switches). This information is used to monitor and correct the behavior of the PC/DNA network, the ASAMs and cbx500s, ASAMs and cbx500 modules, and communication links (physical and logical), and in planning and analysis.
- The ability to establish, view, and change performance thresholds associated with a specific end-user quality of service. The NMS will communicate Performance Management threshold criteria to the ASAMs and NavisXtend provisioning and statistics servers to establish counters for various ATM cell measures.
- Communication of performance and traffic management data to customer management systems to ensure those service objectives (e.g., QOS) are met. The NMS will also perform some limited analysis of the data (e.g., the NMS may associate PVC performance with an affected set of customers).

9.2 Feature Dependencies

Performance Management depends on the existence of a PC/DNA network; nodes (ASAMs, cbx500s, DANAs), interconnecting links (physical and logical), plug-ins, ports, and the presence of the provisioning and statistical EMSs. In particular, this feature depends on the presence of retrieval and event reporting capabilities across the TL1 interface to the ASAMs, and SNMP interface to NavisXtend provisioning and statistical servers. An interface to DANA will be defined at a later date. A user interface is required at the NMS for configuring, information retrieval, and display purposes.

9.3 Feature Description and Flow

Performance Management can be broken down into the following:

- Network performance assessment
- Performance monitoring
- Traffic management and control
- Network data collection.

Figure 9-1 shows the basic Performance Management flow. The process can be described as follows:

- Upon request or periodically the NMS will poll the DSLAMs, NavisXtend statistics server and DANA for performance data. The NMS will communicate to the DSLAMs over the TL1 interface; and to the NavisXtend servers over the SNMP interface.

- NEs and EMSs will respond to the NMS with the requested data.
- The NMS will perform some processing on the received data.
- Based on the information received, the NMS will notify the BBOC and the RPEC (Regional Provisioning Engineering Center) on the nature of the performance information (e.g., data thresholds exceeded "n" times over a given interval).

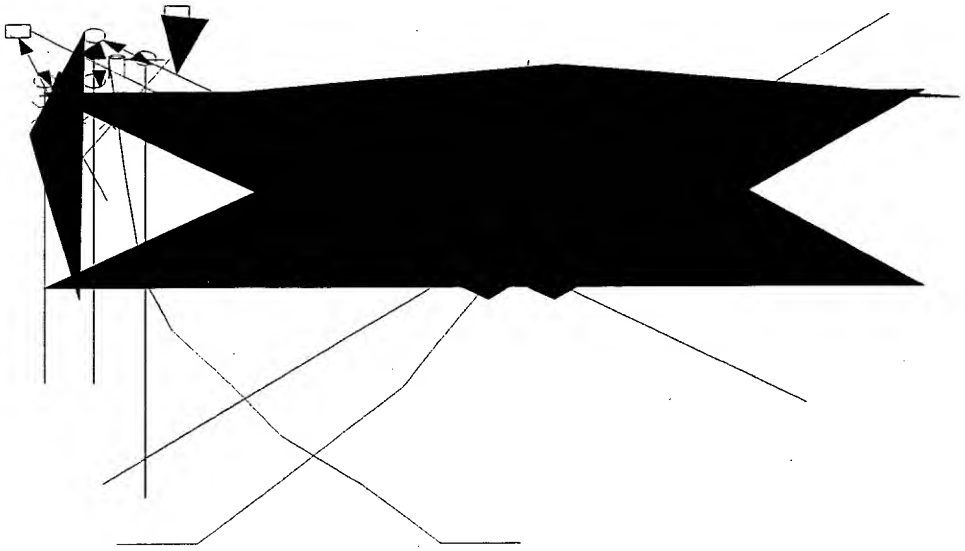

Figure 9-1. Performance Management Process Flow

9.3.1 Network Performance Assessment

The NMS will retrieve DSLAM and ATM switch performance quality and availability parameters -- such as ports in use, utilization data on congestable modules (CPUs, egress buffers, etc.), PVC downtime and link traffic data (cells generated/received, cells loss, AAL5 PDUs sent/received) – from the ASAMs, DANA, and NavisXtend Statistics Server. The NMS shall use this data to evaluate the availability and "service state" associated with the ASAMs, DANA, and cbx500. The NMS will pass this information to a Service Management Function (SMF) that is involved in setting the customer's QOS objectives. This SMF can be part of the NMS or reside in a separate system that is part of the RPEC.

9.3.2 Performance Monitoring

The NMS interacts with the ASAMs over the TL1 interface to retrieve (collect) performance data that it uses to analyze and correlate alarms, events, and traffic across the ASAMs subnetwork -- in the initial phases an ASAM subnetwork is defined by the termination points on the LT cards and NT cards across a single ASAM. The NMS shall

retrieve ATM subnetwork performance data by accessing the NavisXtend Statistics Server via SNMP GetRequests commands. The NavisXtend statistics server may respond immediately (directly) with the data, or it may first query the Network Elements (cbx500s) for the data before responding to the NMS with an SNMP GetResponse. Performance data collected include:

- ASAM common equipment, ATU-C, ATU-R, and software from the AWS
- ATM switches/cross-connects common equipment, line cards, and software from NavisXtend.
- ADSL, SONET, DS3 interface statistics (e.g., LOS, LCD, errored seconds, severely errored seconds, code violations, p-bit coding viloations, p-bit errored seconds, line errored seconds, line code viloations, utilisation, backward/forward ADSL access speed, OAM cells transmitted)
- ATM protocol layer (cells discarded due to HEC violation, cells discarded due to protocol errors, latest occurrence log of discarded cells)
- AAL-5 Protocol layer (invalid fields, CRC-32 violation, reassembly timer expiry)
- UPC/NPC per virtual connection (cells discarded due to UPC/NPC disagreement (CLP = 0+1), cells successfully passed (CLP= 0+1).

9.4 Requirements

9.4.1 General (R2)

PM-NMS-1 The NMS shall allow the user to retrieve performance data over a local GUI. The user shall be able to select a specific NE (CLLI code of ASAM, DANA, cbx500, ATU-R) and a specific port (identified by port_id -- rack/shelf/slot/port-num) on that NE.

PM-NMS-2 The NMS shall allow the user to retrieve data from a list of "record types." Record types shall be:

Current – a real-time display of the current interval (15-minute) data
Totals – historical data for Current Day (the default), Previous Day (96 15-minute periods ago).

PM-NMS-3 The NMS shall automatically retrieve performance data from the ASAMs, DANA, and cbx500 in a configurable interval from 1-60 minutes (default 15 minutes).

PM-NMS-4 The NMS shall timestamp and store any retrieved performance data from the ASAMs (data from COMPLD message) and Cascade provisioning Server (data from SNMP GetResponse) in a local data store for a configurable number of days (default "2" days).

PM-NMS-5 The NMS shall store the data in an ASCII flat file by NE (CLLI code of ASAM, DANA, cbx500; TN for ATU-R) and by interface type (DS3, OC3, VPI/VCI, etc).

PM-NMS-6 The NMS shall notify the user of any errors occurring (e.g., timeouts, DENY, or non-zero instance of SNMP ErrorStatus). Error indications shall indicate the source (CLLI/TID/IPA), message type (PDU type), error_type, and date/time.

PM-NMS-7 The NMS shall clear error notifications upon acknowledgment from the user.

PM-NMS-8 The NMS shall allow a user to activate (enable/disable) the setting of performance thresholds.

9.4.2 ADSL Lines (R2)

PM-NMS-9 The NMS shall periodically and on-demand retrieve performance data for selected ADSL lines. The NMS shall include the TL1 identifier for the group(s) of lines affected.

PM-NMS-10 The NMS shall generate a RTRV-PM-ADSL command to the affected (identified by the tid) set of ADSL lines. The command shall include the following parameters as defined in Section 2.83 of [2]:

- tid
- aid_adsl (rack, shelf, asamCard – type LT, circuit)
- ctag
- monadsl (ADSL Montypes of [2])
- monlev
- locn
- tmpr
- mondat
- montm.

PM-NMS-11 The NMS shall retrieve the current 15-minute count by setting tmpr = "15-Min" and leaving mondat and montm "blank."

PM-NMS-12 The NMS shall retrieve historical totals (current day) default is 32 15-minute counts) on ADSL linecard data by setting tmpr = "15-Min", mondat=All, and montm=All.

ASAMs shall process the RTRV-PM-ADSL command and respond to the NMS as specified in Section 2.83 of [2].

PM-NMS-13 The NMS shall log any negative responses (DENY), received in response to a "RTRV-PM-", from the ASAMs. Error indications shall indicate the source (tid), message type, errorCode and date/time.

9-4

PM-NMS-14 The NMS shall alert the user if the number of DENYs received exceeds a configurable threshold of "noRtrvDeny". The default value for noRtrvDeny is "1".

9.4.3 OC3 Facility (R2)

The NMS will periodically and on-demand retrieve performance data on the OC3 facility that terminates on the ASAM NT card.

PM-NMS-15 The NMS shall retrieve performance data for selected OC3 facilities. The NMS shall include the TL1 identifier for the affected facility.

PM-NMS-16 The NMS shall generate RTRV-PM-OC3 command to the affected (identified by the tid) ASAM OC3. The command shall include the following parameters as defined in section 2.84 of [2]:

- tid
- aid_oc3
- ctag
- monoc3 (OC3 Montypes of []).
- monlev
- locn
- tmpr
- mondat
- montm.

PM-NMS-17 The NMS shall retrieve the current 15-minute count by setting tmpr = "15-Min" and leaving mondat and montm "blank."

PM-NMS-18 The NMS shall retrieve historical totals (current day); default is 32 15-minute counts) on ADSL linecard data by setting tmpr = "15-Min," mondat=All, and montm=All.

ASAMs shall process the RTRV-PM-OC3 command and respond to the NMS as specified in Section 2.84 of [2].

The following requirements apply to the Cascade cbx500s.

PM-NMS-19 The NMS shall retrieve OC3 performance data by generating an SNMP GetRequest to the NavisXtend statistics server. The NMS shall build and construct the GetRequest according to RFC 1157. The message shall include the PC/DNA community name and the IP address of the affected cbx500.

PM-NMS-20 The NMS shall populate the varBindList as follows:

varBindList ::=
SEQUENCE OF
PPort.PPort Id= = CBX ATM OC3 PPort
PPort.PporType= = 4portAtmOC3 STM-1
sonetpmThreshCVSCurrent
sonetpmThreshESSCurrent
sonetpmThreshSESSCurrent
sonetpmThreshCVLCurrent
sonetpmThreshESLCurrent
sonetpmThreshSESLCurrent
sonetpmThreshUASLCurrent
sonetpmThreshCVPCurrent
sonetpmThreshESPCurrent
sonetpmThreshSESPCurrent
sonetpmThreshUASCurrent
sonetpmThreshCVSDay
sonetpmThreshESSDay
sonetpmThreshSESSDay
sonetpmThreshCVLDay
sonetpmThreshESLDay
sonetpmThreshSESLDay
sonetpmThreshUASLDay
sonetpmThreshCVPDay
sonetpmThreshESPDay
sonetpmThreshSESPDay
sonetpmThreshUASDay

Note: The "value" for each of the above corresponding objectNames shall be encoded as "null."

9.4.4 DS3 Facility (R2)

The NMS will periodically and on-demand retrieve performance data on the DS3 facility that terminates on the ASAM NT card.

PM-NMS-21 The NMS shall retrieve performance data for selected DS3 facilities. The NMS shall include the TL1 identifier for the affected facility.
PM-NMS-22 The NMS shall generate a RTRV-PM-T3 command to the affected (identified by the tid) ASAM DS3. The command shall include the following parameters as defined in Section 2.86 of [2]:

- tid
- aid_ds3
- ctag
- monds3 (DS3/T3 Montypes of [2]).

- monlev
- locn
- tmpr
- mondat
- montm.

PM-NMS-23 The NMS shall retrieve the current 15-minute count by setting tmpr = "15-Min" and leaving mondat and montm "blank."

PM-NMS-24 The NMS shall retrieve historical totals (current day); default is 32 15-minute counts) on ADSL linecard data by setting tmpr = "15-Min," mondat=All, and montm=All.

ASAMs shall process the RTRV-PM-DS3 command and respond to the NMS as specified in Section 2.86 of [2].

The following requirements apply to the Cascade cbx500s.

PM-NMS-25 The NMS shall retrieve DS3 performance data by generating an SNMP GetRequest to the Cascade provisioning server. The NMS shall build and construct the GetRequest according to RFC 1157. The message shall include the PC/DNA community name and the IP address of the affected cbx500.

PM-NMS-26 The NMS shall populate the varBindList as follows:

varBindList ::=
SEQUENCE OF
PPort.PPort Id= = CBX ATM DS3 PPort
PPort.PporType= = 8portAtmDS3
ds3pmThreshCVLCurrent
ds3pmThreshESLCurrent
ds3pmThreshSESLCurrent
ds3pmThreshCVPCurrent
ds3pmThreshESPCurrent
ds3pmThreshSESPCurrent
ds3pmThreshSASPCurrent
ds3pmThreshUASCurrent
ds3pmThreshCVCPPCurrent
ds3pmThreshESCPPCurrent
ds3pmThreshSESCPPCurrent
ds3pmThreshSASCPPCurrent
ds3pmThreshUASCPPCurrent
ds3pmThreshCVLDay
ds3pmThreshESLDay
ds3pmThreshSESLDay

ds3pmThreshCVPDay
ds3pmThreshESPDay
ds3pmThreshSESPDay
ds3pmThreshSASPDay
ds3pmThreshUASDay
ds3pmThreshCVCPPDay
ds3pmThreshESCPPDay
ds3pmThreshSESCPPDay
ds3pmThreshSASCPPDay
ds3pmThreshUASCPPDay

Note: The "value" for each of the above corresponding objectNames shall be encoded as "null."

9.4.5 OC12 Facilities (R2)

The following requirements apply to OC12 facilities which terminate on the cbx500s. The far end of these facilities will be terminated at the NSPs.

PM-NMS-27 The NMS shall retrieve OC12 performance data by generating an SNMP GetRequest to the NavisXtend statistics server. The NMS shall build and construct the GetRequest according to RFC 1157. The message shall include the PC/DNA community name and the IP address of the affected cbx500.

PM-NMS-28 The NMS shall populate the varBindList as follows:

varBindList ::=
SEQUENCE OF
PPort.PPort Id= = CBX ATM OC12 PPort
PPort.PporType= = 1portAtmOC12STM-4
sonetpmThreshCVSCurrent
sonetpmThreshESSCurrent
sonetpmThreshSESSCurrent
sonetpmThreshCVLCurrent
sonetpmThreshESLCurrent
sonetpmThreshSESLCurrent
sonetpmThreshUASLCurrent
sonetpmThreshCVPCurrent
sonetpmThreshESPCurrent
sonetpmThreshSESPCurrent
sonetpmThreshUASCurrent
sonetpmThreshCVSDay
sonetpmThreshESSDay
sonetpmThreshSESSDay
sonetpmThreshCVLDay

sonetpmThreshESLDay
sonetpmThreshSESLDay
sonetpmThreshUASLDay
sonetpmThreshCVPDay
sonetpmThreshESPDay
sonetpmThreshSESPDay
sonetpmThreshUASDay

Note: The "value" for each of the above corresponding objectNames shall be encoded as "null."

9.4.6 DS1 Facilities (R2)

The following requirements apply to DS1 facilities that terminate on the cbx500s. The far end of these facilities will be terminated at the NSPs.

PM-NMS-29 The NMS shall retrieve DS1 performance data by generating an SNMP GetRequest to the Cascade provisioning server. The NMS shall build and construct the GetRequest according to RFC 1157. The message shall include the PC/DNA community name and the IP address of the affected cbx500.

PM-NMS-30 The NMS shall populate the varBindList as follows:

varBindList ::=
SEQUENCE OF
PPort.PPort Id= = CBX ATM DS1 PPort
PPort.PporType= = 8portAtmT1
ds1pmThreshESLCurrent
ds1pmThreshCVPCurrent
ds1pmThreshESPCurrent
ds1pmThreshSESPCurrent
ds1pmThreshSASPCurrent
ds1pmThreshCSSPCurrent
ds1pmThreshUASPCurrent
ds1pmThreshESLDay
ds1pmThreshCVPDay
ds1pmThreshESPDay
ds1pmThreshSESPDay
ds1pmThreshSASPDay
ds1pmThreshCSSPDay
ds1pmThreshUASPDay

Note: The "value" for each of the above corresponding objectNames shall be encoded as "null."

9.4.7 ATM Cell Level Protocol Data (R2)

PM-NMS-31 The NMS shall retrieve (from the ASAMs, DANA, and NavisXtend statistics Server) 15-minute current counts and threshold data for *ATM cells discarded due to HEC violations* for incoming cells for each ATM interface (TL1 command and SNMP MIB variables to be defined).

PM-NMS-32 The NMS shall retrieve (from the ASAMs, DANA and and NavisXtend statistics Server) 15-minute current counts and threshold data for *ATM cells discarded due to protocol (header) errors* for each ATM interface. TL1 command and SNMP MIB variables to be defined. For TL1 might be incorporated as part of the RTRV-PM-* command.

PM-NMS-33 The NMS shall retrieve (from the ASAMs, DANA and NavisXtend statistics Server) 15-minute current counts and threshold data for *out of cell delineation anomalies* for incoming cells for each ATM interface. TL1 command and SNMP MIB variables to be defined. For TL1 might be incorporated as part of the RTRV-PM-* command.

PM-NMS-34 The NMS shall set and modify the threshold values for the parameters listed above in ***PM-NMS-31*** through ***PM-NMS-34***. TL1 commands and SNMP MIB variables to be defined.

The ASAMs, DANA, and NavisXtend statistics Server will inform the NMS of any threshold crossings (by virtue of TCAs). The NMS will require the NEs and EMSs to set threshold counters will be set for usage cells, lost cells, and misinserted cells. TCAs, when reported shall include the source (CLLI/TID), time/date, the specific condition, location of the condition, and the specific value.

PM-NMS-35 The NMS shall receive and process TCAs from the ASAMs.

PM-NMS-36 On receipt of a REPT EVT COM, the NMS shall log the occurrence and alert the user. The REPT EVT COM shall be as defined in Section 3.8 of [2].

PM-NMS-37 The NMS shall receive and process (redirected) SNMP Traps (i.e., autonomous notifications) from the NavisXtend provisioning Server (the specific trap definitions are to be defined).

9.4.7.1 AAL5 Protocol Data

Future requirements on the NMS will focus on the retrieval and processing of AAL data from ATM Adaptation layer endpoints. In particular, data will be retrieved from the ATU-R and DANA termination points.

PM-NMS-38 The NMS shall retrieve the following AAL5 performance data from the Dana:

- current, 15-minutes counts of the number of re-assembly timer expirations
- current, 15-minute, counts of the number of CRC-32 violations
- historical (1-96, 15-minute) counts of re-assembly and CRC-32 violation errors. The default value is 32 15-minutes counts.

9.4.7.2 UPC/NPC Monitoring

User parameter control and network parameter control (UPC/NPC) algorithms are used at network elements to police incoming ATM cells to ensure that traffic-generating sources comply with pre-negotiated traffic descriptors. Traffic streams that are non-compliant will result in cells being tagged and/or discarded by the network. Counts of cells discarded by the network can serve as a key component in analyzing and detecting service quality offered by the network.

PM-NMS-39 The NMS shall retrieve, from the ASAM, the current (15-minute) counts of clp=0+1 cells discarded due to traffic descriptor violations per VC link (TL1 command is to be defined).

PM-NMS-40 The NMS shall retrieve, from the NavisXtend statistics Server, the current (15-minute) counts of clp=0+1 cells discarded due to traffic descriptor violations per VC link (SNMP MIB objects to be defined).

PM-NMS-41 The NMS shall retrieve, from the ASAM, historical counts (1-96, 15-minute counts) of clp=0+1 cells discarded due to traffic descriptor violations per VC link. The default is 32 15-minutes counts (TL1 command is to be defined).

PM-NMS-42 The NMS shall retrieve, from the NavisXtend statistics Server, historical (1-96, 15-minute counts) of clp=0+1 cells discarded due to traffic descriptor violations per VC link (SNMP MIB objects to be defined).

PM-NMS-43 The NMS shall retrieve, from the ASAM, the current (15-minute) counts of clp=0+1 cells successfully transmitted per VC link (TL1 command is to be defined).

PM-NMS-44 The NMS shall retrieve, from the NavisXtend statistics Server, the current (15-minute) counts of clp=0+1 cells successfully transmitted per VC link (SNMP MIB objects to be defined).

PM-NMS-45 The NMS shall retrieve, from the ASAM, historical counts (1-96, 15-minute counts) of clp=0+1 cells successfully transmitted per VC link. The default is 32 15-minutes counts (TL1 command is to be defined).

PM-NMS-46 The NMS shall retrieve, from the NavisXtend statistics Server, historical (1-96, 15-minute counts) of clp=0+1 cells successfully transmitted per VC link (SNMP MIB objects to be defined).

PM-NMS-47 The NMS shall set and modify the threshold values for the parameters listed above in ***PM-NMS-39*** through ***PM-NMS-46*** (TL1 commands and SNMP MIB objects to be defined).

PM-NMS-48 The NMS shall be able to activate/deactivate UPC/NPC monitoring on a specific (set of) VC links (TL1 commands and SNMP MIB objects to be defined).

PM-NMS-49 To support trending (i.e., to predict failure or degraded conditions), the NMS shall be able to set periodic intervals for the autonomous reporting of performance information by the EMSs, DANA, and ASAMs (TL1 commands and SNMP MIB objects to be defined).

9.4.8 VP/VC Performance Data

Since PVCs are provisioned from the ATU-R to DANA and in some cases from the ATU-R to the NSP (ISP) it might become necessary overtime to collect data related to the actual PVC performance. Example of this information might be counts on the number of cells sent, lost, and misinserted.

PM-NMS-50 The NMS shall be required to retrieve and change the thresholds of each of the registers associated with each of the cells sent, cells lost, and misinserted cells.

PM-NMS-51 The NMS shall require the ASAMs, DANA and NavisXtend statistics Server to set threshold counters for usage cells, lost cells, and misinserted cells.

9.5 Traffic Management and Control

9.5.1 Description

The initial PC/DNA service will be offered with PVCs over which a UBR service is provisioned on each VCL. As a consequence, ATM termination points at NEs will be required to set the CLP bit in the cell header to "1." The NMS Performance Management function will be required to convey to the configuration management function (planning and engineering) the UPC/NPC cell discarded parameter values. Configuration management can then take the necessary steps to alleviate congestion (e.g., re-assign VCLs to different VPLs).

9.6 Issues

The following are some outstanding issues:

- Interfaces from the NMS to DANA needs to be defined. Message exchange and elements of procedures associated with facility performance, ATM cell level protocol data, and PVC performance should be part of this interface definition.
- TL1 commands for ATM/AAL related performance data needs to be defined. This requires discussion with Alcatel SMEs.

9-14

10. Security Management

10.1 Purpose

The Security Management feature of the FastAccess NMS is primarily concerned with maintaining system integrity by preventing

- Unauthorized individuals or systems from accessing the NMS data, functions, or system, and
- Authorized users (operators or systems) from performing functions beyond their scope of responsibility.

In addition, the NMS may be responsible for acting as a central point of administration for managing the security of NEs (e.g. DSLAMs) and EMS (e.g. AWS), including password and access control.

10.2 Dependencies

This feature is closely coupled with:

- The GUI command set
- The system interfaces between the NMS and SOCS, AWS, NavisCore, and the Service Gateway
- The security capabilities of the NEs and EMSs.

10.3 Feature Description and Flow

The system security set of features should be constantly operational. Management of security features for NEs and EMSs will be restricted to authorized users on an "as needed" basis.

10.4 Requirements (R1)

SM-NMS-1 The FastAccess NMS should ensure multiple levels of security are maintained, including:

- System authorization and authentication controls;
- Operator authorization and authentication controls;

System authorization and authentication deals with basic access to the operating system on which the NMS resides (e.g., UNIX). Operator authorization and authentication deals with controlling access to the NMS, and ensuring that users are only allowed to perform actions consistent with their level of responsibility or authority.

SM-NMS-2 **Operating System-level security:**
The NMS *shall* operate on a platform that includes facilities for:

- Logging login attempts
- Encrypting passwords
- Denying access after a pre-set number of incorrect login attempts
- Aging passwords.

SM-NMS-3 **NMS-level Access Security:**
The NMS *shall* include facilities for:

- Assigning/maintaining operator logins and passwords on a per-operator basis
- Logging operator actions
- Enabling limits to be placed on individual operator access to actions by any or all of
- Application groups
- Individual commands
- Network partitions
- Specific managed objects.

Assignment and maintenance of operator logins/passwords, as well as enabling or disabling access to specific NMS features, are functions enabled via the NetExpert Authorization Editor. Logging of operator activity is generic to the NetExpert framework. As the Authorization Editor tool allows a systems administrator to customize these settings in the runtime system, it is recommended that these functions be established late in the development/testing cycle, with benefit of some 'hands-on' use by the (future) users and administrators.

SM-NMS-4 **Additional Security Management Requirements:**
As per the OTP [1], the NMS is required to administer the security of certain network elements and element management systems. This includes the ability to:

- Report on all NE security violation events (as received from the DSLAM, Ascend Fault Server, and Service Gateway)
- Retrieve security data from NEs
- Remotely set up NE user accounts with appropriate privileges
- Retrieve and change passwords associated with individual NEs.

Access to these functions is expected to be tightly controlled (e.g., Superuser access only).

NE (or EMS) security violations that are reportable via the EMS/NMS interface can be tracked as system 'events,' and specific Alert Display filters can be developed to isolate and monitor these events. DSLAM user accounts and passwords can be set via the NMS using the TL1 command set. The ability to change/reset all NE passwords with one single menu command can be achieved in rules, by creating rules that loop through all known DSLAMs and reset the passwords via the TL1 SET-xxxx-yyyy command.

11. NMS External Interfaces

As Figure 2-3 depicts, the NMS interfaces to a variety of systems for the execution of provisioning, inventory, fault, and Performance Management functions. Some of these systems are peer OSs while others are the NEs themselves. The variety, type, and placement of these systems dictate the interfaces supported at the NMS. For example, when interfacing to peer OSs in existing work centers, the interfaces are typically based on TCP/IP and /or X.25 – the incumbent interfaces of our legacy environment. A similar observation can be made for application layer interactions that are characteristically SNMP, and to a lesser extent, Transaction Language – 1 (TL1).

Figure 2-3 shows that the NMS functional interactions occur across the following interfaces:

- NMS – AWS
- NMS – DSLAMs
- NMS – NavisXtend (NavisXtend PS, NavisXtend FS, and NavisXtend SS (R2))
- NMS – NMA
- NMS – SOCS.

11.1 NMS – AWS Interface (R1)

11.1.1 NMS/AWS Connection Management (R1)

11.1.1.1 Purpose

The purpose of this feature is to manage the operations of the NMS/AWS links that are used to carry configuration, fault, performance, and security management messages between NMS and subtending AWSs. Although the underlying transport protocols X.25 protocol can identify when the NMS/AWS link is down, the focus here is on the application requirements.

11.1.1.2 Dependencies

None.

11.1.1.3 Feature Flow

The DSLAM TL1 interface is remoted via ATM inband channels to the AWS. At the AWS, a "gateway" consolidates all the DSLAM TL1 messages and provides three virtual channels to upstream OSs such as NMA, NMS, or others. Each of these channels can be used for all the TL1 messages, autonomous, and command/response. The only function of the "gateway" is to look at the TIDs of the received messages and forward them to the appropriate DSLAM. The TL1 is a "pass-through" interface and AWS applications are

not used. However, any operations on a DSLAM through the TL1 message generates a "report database change" message by the DSLAM that is automatically sent to AWS via the SNMP interface so that the AWS database is updated.

The FastAccess NMS may use "two" virtual circuits from each AWS, one to receive the DSLAM *autonomous* alarm and event messages, the other to be used for *command/response* mode.

The following flow may be used to receive "autonomous alarm/event" messages using the first of the AWS/NMS virtual channel:

1) NMS will issue an ACT-USER command to login to a specific DSLAM. This message includes user ID and password. Normally, this function is automatically done by NMS when it comes up.
2) To keep the session up with the DSLAMs, NMS will periodically issue a keep alive signal by using the RTRV-HDR command. Once every 15 minutes per DSLAM is recommended.
3) To terminate a user session with a DSLAM (i.e., log-off), the CANC-USER command may be used. This command enables a user with Superuser privilege to terminate another user session.

The following flow may be used for "command/response" messages using the second AWS/NMS virtual channel:

1) NMS *may* issue an ACT-USER command to login to a specific DSLAM. This message includes user ID and password. *Note:* Some of the AWS TL1 commands may be provisioned to automatically perform the function of ACT-USER command as a part of those commands. Hence, for "certain commands" there is no need to issue a separate ACT-USER command. For example, all the RTRV-XXX commands (not including the security commands) can be provisioned to behave this way. Hence, to log in to a DSLAM, either ACT-USER will be used before issuing the actual command, or a command that includes ACT-USER functions will be used.
2) To keep this channel only for command/response mode, NMS will issue an INH-MSG-ALL command to inhibit all autonomous messages below the specified severity level (e.g., critical). The INH-MSG-ALL will stay in effect as long as the session is on.
3) If ACT-USER command is automatically initiated when NMS comes on, to terminate a user session with a DSLAM (i.e., log-off), the CANC-USER command may be used.

11.1.1.4 Requirements

INT-NMS-1 NMS shall be able to automatically "log on/off" to one, all, or a specified subset of DSLAMs by using one command (i.e., using variation of ACT-USER/CANC-

USER). Grouping and ranging across DSLAMs shall be supported by for these commands.

INT-NMS-2 To keep a session alive with DSLAMs on the autonomous channels, the NMS shall automatically and periodically (once every 15 minutes per NE is recommended) send a keep alive signal to DSLAMs. This keep alive signal shall be implemented via the RTRV-HDR command. Grouping and ranging across DSLAMs shall be supported for this command.

The NMS interfaces to Alcatel's AWS in a pass-through mode of operation. That is, the AWS performs skeletal processing and terminates only the lower layers (X.25 data transfer phase [DTP], link, and physical layers) of the protocol stack shown in Table 11-1. The TL1 application is routed via a gateway at the AWS where it is multiplexed onto an ATM permanent virtual connection to a selected DSLAM -- identified by the TL1 Target Identifier (TID) parameter.

Table 11-1. NMS – AWS Protocol Stack

TL1*
X.25 DTP
ISO 7776
RS 449

* - indicates virtual transport only.

INT-NMS-3 The NMS shall implement the protocol stack shown in Table 11-1 for communicating to the AWS.

INT-NMS-4 The NMS shall terminate and process X.25 data transfer packets consistent with the elements and procedures expected over the BellSouth X.25 Operations Network. In communicating to an AWS, the NMS shall use a maximum of "n" X.25 permanent virtual circuits provisioned to the selected AWS. "N" is a configurable parameter in the range of 0-3 (decimal); the default value shall be 2.

The NMS may use the two virtual circuits from an AWS as such; the one to receive DSLAM *autonomous* alarm and event notification messages. The other to be used bi-directionally in a *command/response* mode.

11.1.1.5 Notes, Issues, and Questions

1) Does ACT-USER command have an associated timer that will expire? What kind of timer is supported?

11.2 NMS – DSLAM Interface (R1)

The NMS communication to the DSLAM is limited to the TL1 application. As mentioned in the previous section, the TL1 application layer is transparent to the AWS and actually terminates on the NMS and DSLAMs. The TL1 layer is encapsulated in X.25 packets between the NMS and the AWS. Between the AWS and the DSLAM it is encapsulated in ATM cells.

INT-NMS-5 The NMS shall terminate and process TL1 commands/responses as specified in the Alcatel TL1 specification.

INT-NMS-6 The NMS shall populate the TID in command messages with the value of the CLLI code for the selected DSLAM.

A DSLAM receiving an NMS-generated command will process and respond only if the TID matches its Site Identifier (SID). The DSLAM will include its SID as part of the response.

INT-NMS-7 The NMS shall set the CTAG to a value in the range from 1- 999999 (decimal). The NMS shall increase this number sequentially for each new command transmitted. The NMS shall use this CTAG and the value of the SID, of the responding DSLAM, to validate responses.

INT-NMS-8 The NMS shall discard acknowledgments/responses with an invalid CTAG and /or SID values.

The NMS must be provisioned with the CLLI code of all DSLAMS within its domain. At the AWS, a table shall exist that maps CLLI codes (TIDs) to a given ATM virtual connection.

11.3 NMS – NavisXtend Interfaces (R1)

11.3.1 NavisXtend/NMS Connection Management (R1)

11.3.1.1 Purpose

The purpose of this feature is to manage the operations of the NMS/NavisXtend Provisioning/Fault Servers links that are used to carry configuration and fault management messages between NMS and those Servers.

11.3.1.2 Feature Flow

Unlike the AWS TL1 interface, which is based on the X.25 connection oriented protocol, the links from NMS to NavisXtend Provisioning and Fault Servers are IP-based and hence, connectionless. Therefore, there is no connection to manage, no login/logoff and no keep alive signal. To forward the SNMP traps from the Fault Server to NMS, the IP address of the NMS must be specified in the Fault Server. Also to send SNMP commands from NMS to the Provisioning Server, the IP address of the Provisioning Server must be specified in NMS.

11.3.1.3 Requirements

INT-NMS-9 To establish communications between the NMS and NavisXtend Fault and Provisioning Servers, appropriate IP addresses must be incorporated.

The NMS interfaces to the NavisXtend family of servers via the protocol stack shown in Table 11-2. The interfaces to NavisXtend Provisioning and Statistics (R2) servers are bi-directional. The interface to NavisXtend Fault Server is uni-directional, from the server to the NMS, and is used to convey SNMP traps only. The provisioning server enables NMS to provision a "subnetwork connection" across the Ascend ATM subnetwork. The Statistics server enables the NMS to garner performance monitoring data and for the setting of performance thresholds. The NMS shall be provisioned with the valid IP addresses of all the NavisXtend servers.

Table 11-2. NMS – NavisXtend Servers Protocol Stack

RFC 1157 (SNMP)
X.209 (BER)
RFC 768 (UDP)
RFC 791 (IP)
IEEE 802.3/802.2
Ethernet

INT-NMS-10 The NMS shall implement the protocol stack shown in Table 11-2 for communicating to the NavisXtend Provisioning, Fault, and Statistics Servers.

INT-NMS-11 The NMS shall terminate and process SNMP PDUs consistent with the elements and procedures defined in Section 4 of the Ascend Provisioning Server Users Guide.

INT-NMS-12 The NMS shall send/receive SNMP commands/responses over UDP port 161. The NMS shall receive SNMP traps over UDP port 162.

INT-NMS-13 The NMS shall communicate with the NavisXtend servers using an SNMP authentication and access policy based on the "FastAccess" community name. This name is coded as an octet string.

INT-NMS-14 The NMS shall validate SNMP GetResponse and Trap messages according to RFC 1157 and the procedures outlined in Section 4 of [3]. The NMS shall discard the PDU and log the error if any of the following occurs:

- Inability to parse the PDU
- Invalid SNMP version number
- Invalid Community name
- For GetResponse, invalid RequestId.

INT-NMS-15 The NMS shall notify the user of any errors (e.g., timeouts), non-zero instance of ErrorStatus, or items defined in **INT-NMS-11**. Error indications shall indicate the source (CLLI/IPA), PDU type, error_type, and date/time.

11.4 NMS – NMA Interface (R1)

The NMS interfaces to NMA via the protocol stack shown in Table 11-3. From an application (TL1) perspective the interface is uni-directional – from NMS to NMA. NMS uses this interface to convey the Fault management information received from the DSLAMs. The NMS shall be provisioned with the valid IP address for NMA.

Table 11-3. NMS – NMA Protocol Stack

TL1
RFC 793 (TCP)
RFC 791 (IP)
IEEE 802.3/802.2
Ethernet

INT-NMS-16 The NMS shall implement the protocol stack shown in Table 11-3 for communicating to NMA. The TL1 interface shall be as specified in Section 11.2.

11.5 NMS – SOCS Interface (R1)

The NMS supports an interface to SOCS for "flow-through" provisioning of FastAccess service orders (SOs). This interface is bi-directional and the NMS will support the protocol stack shown in Table 11-4. The NMS shall be provisioned with the valid addresses (IPAs, CLLIs) for the various SOCS machines.

Table 11-4. NMS – NMA Protocol Stack

SocsNMSApp
Navigator
BOSIP (TCP/IP)
Ethernet

INT-NMS-17 The NMS shall implement the protocol stack shown in Table 11-4 for communicating to SOCS.

The SocsNMSApp will be encapsulated within a *Navigator Contract*. SOCS will identify FastAccess SOs by a unique Field ID (FID ***ADSL***. All SOs with the *ADSL* FID with an I or O action will be routed to the NMS. In addition, each occurrence of select status changes to the SOs will also be routed to the NMS. The valid status changes on a SO are Cancel (CA), Pending (PD), and Completion Pass (CP).

11.5.1 SocsNMSApp

SocsNMSApp is an acknowledged communication process between SOCS and the NMS. SOCS passes SOs, on receipt from upstream systems, to the NMS. The NMS is required to acknowledge the successful receipt of all SocsNMSApp PDUs. The process is as follows:

1. SOCS receives SOs with FID of *ADSL* with an I or O action from provisioning systems (e.g., SOAC, BASS, CRIS). The SO contains the following information:
   - FID of *ADSL*
   - Physical facility assignment: loop, DSLAM port
   - SO number and type (e.g., residential or business; new-connect, change, service denied, restore, or disconnect)
   - SO status change (e.g., cancel, pending, completion pass)
   - Customer ID (e.g., telephone number)
   - Customer name and address
   - Attributes of FastAccess service, if applicable (e.g., quality of service (QOS) specifications, guaranteed minimum speed)

- Requested NSP IDs for those services going through the Service Gateway.
- For services involving direct connection to the NSP, the Circuit ID terminating at the NSP and the associated VPI/VCIs
- Preferred link information (e.g., virtual connection ID) supplied by an NSP (this applies to business FastAccess SOs when the NSP is a Corporate LAN and has multiple links to BellSouth's ATM sub-network)
- DSLAM port assignment from COSMOS or R-DSLAM assignment from LFACS
- Due date.

2. The SocsNMSApp (at SOCS) appends the SOCS-HEADER (Order-number, Sequence-number-resend, Application-ID == NMS, IMS-userId, Initial-date and Operator-Id). The second character of the order-number represents the SOCS site. The sites and encoding of the second character of the order-number are as follows:

IMS Region	Site	2nd Character of Order Number
ARC	Atlanta	O
AFS	Macon	P
B04	Tennessee	9
C04	Mississippi	6
D04	Alabama	1
E04	Louisiana	5
G04	Kentucky	4
JRC	Jacksonville	Y
MRC	Miami	Q
MFS	Ft Lauderdale	R
RRC	North Carolina	X
RFS	North Carolina	W

3. The SocsNMSApp then forwards this SocsNMSApp PDU, via the Navigator client, to the NMS.
4. The SocsNMSApp at SOCS will resend the PDU if an acknowledgment is not received within a configurable time period (provisionally set at 240 mins). The PDU will be resent up to a maximum of "n" times (the default value of "n" is set at 5).

5. The SocsNMSApp at the NMS generates a response to the received PDU. The response will contain the following:
   - Return-code = '0000' (successful receipt)
   - Order-number = value of 'Order-number' received
   - Sequence-number-re-send = value of 'sequence-number-re-send' received
   - Application-Id = 'NMS'.

INT-NMS-18 The NMS shall discard the SO (SocsNMSApp PDU) if any of the following occurs:
- Invalid order-number (e.g., invalid site sub-field)
- Invalid sequence-number-re-send (i.e., value greater than '05')
- Invalid application-id (value other than 'NMS')
- Invalid IMS-userid.

INT-NMS-19 The SocsNMSApp at the NMS shall acknowledge receipt of the SO (SocsNMSApp PDU) upon successful validation of SO data. The NMS shall respond with the following:
- Return-code (4 bytes) == '0000'
- Order-number (8 bytes) == value of 'Order-number' received
- Sequence-number-re-send (2 bytes) == value of 'sequence-number-re-send' received
- Application-Id (3 bytes) == 'NMS'.

The NMS will process the SO information as Section 6 defines.

INT-NMS-20 All FastAccess service orders received by the NMS shall have the customer's name, address, and telephone number.

INT-NMS-21 All FastAccess service orders received by the NMS shall have the following service-related information: Type of service order (new-connect, disconnect, or change order); "Due Date," and "Class of Service" identified by its *ADSL* FID.

INT-NMS-22 All FastAccess service orders received by the NMS shall include a DSLAM (or R-DSLAM) port assignment in COSMOS/LFACS naming convention.

INT-NMS-23 Consumer-class Tier 1 FastAccess service orders received by the NMS shall have the NSP ID and address of the NSP.

INT-NMS-24 Consumer-class Tier 2 FastAccess service orders received by the NMS shall have NSP IDs and addresses of multiple NSPs.

INT-NMS-25 Business-class "best-effort - no guarantees' FastAccess service orders received by the NMS shall have the name and address of the NSPs.

INT-NMS-26 Business-class "minimum bandwidth guaranty" FastAccess service orders received by the NMS shall have the following information besides the NSP ID and address of the NSP: Physical circuit ID for the physical link between the NSP and ATM switch with associated VPI/VCI.

11.5.2 Navigator Contract

Navigator is a BellSouth protocol application suite providing messaging, routing, and transaction services to BellSouth OSs (*Navigator* details can be found at www.navigator.bst.bls.com). *Navigator* provides distributed access over UNIX platforms. *Navigator* software provides client-server interfaces based on predefined *contracts*.
Navigator exists at potentially three types of subsystems: client; service broker; and server. In typical implementations, the broker resides on the same platform as the server. Brokers are used in "dynamic" routing. Servers are requested to register their service capabilities with this broker. The server must provide its name, network address, IID (Interface ID) and Service Name. The IID represents the system (e.g., "NMSFA@DEV" – for FastAccess NMS application used in the production system), and the Service name represents the application process on that system (for FastAccess, the Service Name will be FAPROV – for FastAccess provisioning process). Once a server registers with the broker, the broker will route any subsequent client (i.e., SOCS) requests for a particular service to the registered server (i.e., NMS) process. Navigator contracts (services) are defined by the NMS. The service definition constitutes a Contract Name, Contract Version, Routing Key, Process Mode, and message data.

The process mode provides the flexibility to use the same contract in different environments such as development, testing, or production.

Navigator contracts for the FastAccess NMS provisioning service will be dynamically routed.

INT-NMS-27 The NMS shall implement the Navigator broker application.

INT-NMS-28 The NMS shall implement the Navigator server application.

INT-NMS-29 The NMS shall implement the Navigator contract with the following:

- The *contract_name* shall be encoded as "NMSFASOC"
- The *contract_type* shall be "fixed key distributed (4)"
- The *version_release* shall be encoded as "0001"
- The *input_fmt* shall be encoded as "variable"
- The *response_fmt* shall be encoded as "fixed".

The fields in the contract flags shall be as follows:

- *def_vers_ind* encoded as "1"
- *update_ind* encoded as "0"
- *response_ind* encoded as "1"
- *queueing_ind* encoded as "0"
- *null_ind* encoded as "0"
- *dynamic_routing* encoded as "1"
- *compress_input* encoded as "0"
- *compress_output* encoded as "0".

Routing rules for the navigator contract will be based on ProcModes. Associated with each of the defined ProcModes will be an IID that points to the system to which the contract should be routed.

- The valid ProcModes shall be:
  - D Development
  - P Production
  - R Training
  - S System Test
  - T Test.
- The valid IIDs shall be:
  - NMSFA@DEV
  - NMSFA@PROD
  - NMSFA@TRAIN
  - NMSFA@SYS
  - NMSFA@TEST.
- The *service-name* used in all FastAccess NMS provisioning Navigator contracts shall be "FAPROV."
- The *process layer Interchange Code* shall be "B" (both ASCII and EDCDIC).
- The *key parsing rules* shall be as defined in Table 11-5.

Table 11-5. Key Parsing Rules

Rule Seq. Num	Key Seg. Offset	Key Seg. Length
1	0	0

- The *routing rules* shall be as defined in Table 11-6.

Table 11-6. Routing Rules

Entry no	Low Key	High Key	IID	Service	Tran
1	D	D	NMSFA@DEV	FAPROV	
2	P	P	NMSFA@PROD	FAPROV	
3	R	R	NMSFA@TRAIN	FAPROV	
4	S	S	NMSFA@SYS	FAPROV	
5	T	T	NMSFA@TEST	FAPROV	

- The *input data exchange unit* shall be as defined in Table 11-7.

Table 11-7. The IDU Section Variables

Sequence	Name	Picture
1	See SO Reference Document	X(60000)

- The *output data exchange unit* shall be as defined in Table 11-8.

Table 11-8. The ODU Section Variables

Sequence	Name	Picture
1	See SO Reference Document	X(17)

- The *contract clients* shall be as defined in Table 11-9.

Table 11-9. Contract Clients

Client Name	Client Description
SOCS	Service Order Control System

- The I/O attributes shall be as follows:

I/O Attributes

Type	Level	Name	Entity	Picture
I	1...	***SOCS-HEADER***		
I	.2..	ORDER-NUMBER	SOCS HEADER	X(8)
I	.2..	SEQUENCE-NUMBER-RESEND	SOCS HEADER	9(2)
I	..3.	(00-99)	SOCS HEADER	
I	.2..	APPLICATION-ID	SOCS HEADER	X(3)
I	..3.	(NMS)	SOCS HEADER	
I	.2..	IMS-USERID (CUID)	SOCS HEADER	X(8)
I	.2..	INITIAL-DATE (CCYYMMDD)	SOCS HEADER	
I	..3.	INITIAL-YEAR (CCYY)	SOCS HEADER	X(4)
I	..3.	INITIAL-MONTH (MM)	SOCS HEADER	X(2)
I	..3.	INITIAL-DAY (DD)	SOCS HEADER	X(2)
I	..3.	INITIAL-TIME (HHMMSS)	SOCS HEADER	X(6)
I	.2..	OPERATOR-ID	SOCS HEADER	X(5)
I	1...	***SERVICE_ORDER_INFORMATION***		
I	.2..	**FIELDED_IDENT**	SERVICE ORDER NFORMATION	
I	..3.	FULL_STATUS	SERVICE ORDER INFORMATION	
I	...4	PREFIX	SERVICE ORDER INFORMATION	X
I	...4	STATUS	SERVICE ORDER INFORMATION	X(2)
I	...4	SUFFIX	SERVICE ORDER INFORMATION	X
I	..3.	SWITCHING_NPANXX	SERVICE ORDER INFORMATION	X(6)
I	..3.	ROUTING_CODE	SERVICE ORDER INFORMATION	
I	...4	GEN_CLASS_OF_SERVICE	SERVICE ORDER INFORMATION	X
I	...4	WORK_FUNCTION_CODE	SERVICE ORDER INFORMATION	X
I	..3.	SUPP_ROUTING_CODE	SERVICE ORDER INFORMATION	X
I	..3.	HN_PURGE_DATE	SERVICE ORDER INFORMATION	X(8)
I	...4	(CCYYMMDD)	SERVICE ORDER INFORMATION	
I	..3.	SUPPLEMENTAL_NPA_NXX	SERVICE ORDER INFORMATION	X(6)
I	..3.	SPECIAL_ORDER_IND	SERVICE ORDER INFORMATION	X
I	..3.	TIRKS_IND	SERVICE ORDER INFORMATION	X
I	..3.	AUTOMATIC_COMPETIONS_IND	SERVICE ORDER INFORMATION	X
I	..3.	BYPASS_FACS_IND	SERVICE ORDER INFORMATION	X
I	..3.	ROUTING_SEGMENT	SERVICE ORDER INFORMATION	X
I	..3.	TELE_NUMBER	SERVICE ORDER INFORMATION	
I	...4	TELE_AREA	SERVICE ORDER INFORMATION	X(4)
I	...4	TELE_NPA_NXX	SERVICE ORDER INFORMATION	X(8)
I	..3.	SPECIAL_ACTION_IND	SERVICE ORDER INFORMATION	X
I	..3.	CUSTOMER_CODE	SERVICE ORDER INFORMATION	X(3)
I	..3.	COMPLETION_DATE	SERVICE ORDER INFORMATION	X(8)
I	..4	(CCYYMMDD)	SERVICE ORDER INFORMATION	
I	..3.	EXCHANGE_CODE	SERVICE ORDER INFORMATION	X(4)
I	..3.	APPLICATION_DATE	SERVICE ORDER INFORMATION	X(8)
I	...4	(CCYYMMDD)	SERVICE ORDER INFORMATION	
I	..3.	HANGUP_TIME	SERVICE ORDER INFORMATION	X(4)
I	...4	(HHMM)	SERVICE ORDER INFORMATION	
I	..3.	ISSUE_DATE	SERVICE ORDER INFORMATION	X(8)
I	...4	(CCYYMMDD)	SERVICE ORDER INFORMATION	
I	..3.	SERV_ORDER_NUM	SERVICE ORDER INFORMATION	X(8)
I	..3.	ORDER_NO_CORRECT_SUFFIX	SERVICE ORDER INFORMATION	X
I	..3.	FILLER	SERVICE ORDER INFORMATION	X(4)
I	..3.	CLASS_OF_SERVICE	SERVICE ORDER INFORMATION	X(5)
I	..3.	SALES_CODE	SERVICE ORDER INFORMATION	X(7)
I	..3.	DUE_DATE	SERVICE ORDER INFORMATION	X(8)
I	...4	(CCMMYYDD)	SERVICE ORDER INFORMATION	
I	..3.	ACCESS_CODE	SERVICE ORDER INFORMATION	X
I	..3.	APPOINTMENT_CODE	SERVICE ORDER INFORMATION	X
I	..3.	MISSED_APPOINTMENT_CODE	SERVICE ORDER INFORMATION	X
I	.2..	**SECTIONS_OF_SERVICE_ORDER**	**SERVICE ORDER INFORMATION**	**X(500000)**
I	..3.	(SECTIONS OF THE SERVICE	SERVICE ORDER INFORMATION	

```
I    ..3.    ORDER WILL APPEAR IN THE     SERVICE ORDER INFORMATION
I    ..3.    FOLLOWING ORDER IF THEY      SERVICE ORDER INFORMATION
I    ..3.    EXIST)                       SERVICE ORDER INFORMATION
I    ..3.    UNFIELDED_IDENT/LIST         SERVICE ORDER INFORMATION
I    ..3.    CONTROL                      SERVICE ORDER INFORMATION
I    ..3.    DIRECTORY                    SERVICE ORDER INFORMATION
I    ..3.    TRAFFIC                      SERVICE ORDER INFORMATION
I    ..3.    BILL                         SERVICE ORDER INFORMATION
I    ..3.    SERVICE_AND_EQUIPMENT        SERVICE ORDER INFORMATION
I    ..3.    REMARKS                      SERVICE ORDER INFORMATION
I    ..3.    ASSIGNMENT                   SERVICE ORDER INFORMATION
I    ..3.    STAT                         SERVICE ORDER INFORMATION
I    ..3.    NOTE                         SERVICE ORDER INFORMATION
I    .2..    ROUTING_SUB                  SERVICE ORDER INFORMATION
I    ..3.    (CABS_DESIGN_ONLY_AND_MUST   SERVICE ORDER INFORMATION
I    ..3.    APPEAR_LAST)                 SERVICE ORDER INFORMATION
I    .2..    END_ORDER_IND(HEX_0C)        SERVICE ORDER INFORMATION X
O    1...    RETURN-CODE                                            X(4)
O    .2..    (0000)
O    1...    ORDER-NUMBER                                           X(8)
O    1...    SEQUENCE-NUMBER-RESEND                                 9(2)
O    1...    APPLICATION-ID                                         X(3)
O    .2...   (NMS)
```

- The *Completion Codes* shall be as defined in Table 11-10.

Table 11-10. Completion Codes

Code	Description
0000	Normal Completion

12. Open Issues/Questions

12.1 Service Order Open Issues

The following is a list of issues concerning items of information that NMS needs from the different Service Orders that will support FastAccess services. These items of information are needed to populate the NMS database and for the logical part of the provisioning process for Fast Access services.

The comments and resolution of service order-related issues for NMS based on our meeting with Sheri O'dell were presented to Joan Teer's Customer Team on The team agreed with many of the proposed resolutions for these issues while other issues still remain to be worked out. Section 12.1.1 lists issues that have been resolved, Section 12.1.2 lists issues with resolution that may be subject to modification as indicated and Section 12.1.3 lists issues that are still open.

12.1.1 Resolved Issues

1. Which USOC should NMS use when parsing the SO. Should NMS take the basic class of service or the USOC from the Header section or from the S&E section, or does it matter, will it always be the same?

NMS must use the ADLXX USOC from the S&E section of the Service Order, where XX represents the category and tier of service. This is a preliminary proposal (see Section 12.1.2).

2. Which is the correct section (List or Bill) to parse the Customer name to be stored in NMS?

The customer name must be retrieved from the List section followed by the LN, NP or NLST FID.

3. What is the FID for a listed telephone # in the List section? Can this field be used, or should the telephone number in the Header section be used?

If NMS needs to derive the customer name from the List section, it would be nice to use the telephone # from there as well. The TN number must be derived from the S&E section following the ADL USOC.

4. Should the "ISA" FID for the street address in the List section be used in NMS for the customer address?

Yes, the SA FID provides the customer address.

5. How do you recognize a cancellation of FastAccess service only? Will this be a disconnect order, or a change order to delete only the FastAccess service?

It will be a C order type with an "O" suffix associated with the ADSL FID and equipment codes that need to be disconnected.

6. Will Record orders be sent to NMS for updates to the customer address? What other updates will NMS need from a record order? Change service type? PVC change?

NMS will get Record order types with an I or an O ADSL FID in the SO Header. Changes in the List section should be handled by NMS (customer name, address). If "I" or "O" ADL in the S&E section, NMS should RMA.

7. In the S&E section of a Business SO, the /RMKR floating FID contains the VPI/VCI and also the NSP provider. Are these in the same place all the time and are they in fixed lengths? We need to know how we can identify this information in the remarks.

The RMKR field will not be used. The S&E section will contain a floating FID VPI and FID VCI which will be present for Category 3 only. A proposed floating NETP FID followed by the quantity will be used to identify the NSP(s).

8. On business SOs that don't go through the gateway, is there a FID to identify the required VPI/VCI? If so, what section will it be in?

Yes, FID VPI exists today (includes VCI). Resides in S&E section.

9. When an update to a pending order (to make a correction)is sent for any order type, can we assume that the previous order can be deleted and replaced with the updated order?

Yes.

10. If a business customer calls for 30 customers to be installed, are there 30 separate SOs or only one SO?

Yes (to one or thirty?).

11. How will SOCS identify service orders that need to be sent to NMS?

The presence of an I or an O ADSL FID in the header section will be used by SOCS to identify orders that need to be sent to NMS. *It does not indicate the category and tier of service.*

12. NMS will need to read the SOCS status in the fielded Header section of the service order for processing.

The following SOCS status must be read:
CP for completion
CA for cancel
PD for pending.

12.1.2 Subject to Modification

1. We need the USOC that will be used for each Tier of service for Consumer and Business. NMS will use these USOCs to map to the appropriate profiles for the class of service.

USOCs to be used for ADSL-based services are not finalized yet. Current proposal is to use ADLXX, where XX represents category and Tier (e.g., ADL11 means Category 1, Tier 1 service)

[This resolution is based on the Draft Tariff Proposal for ADSL Platform-based services and may be modified in line with the final Tariff proposal]

2. Is the floating FID "AR" always associated with a COSMOS/DSL assignment?

No. Use of proposed "GF" FID will be used.

[The creation of "GF" FID is being pursued with Bellcore]

3. Will all new ADSL orders for existing POTS customers be Change orders? If yes, how do we distinguish this type of order from "change orders" that are issued after completion?

Yes, NMS will need to verify if customer record already exists. If it does, this will be a change to existing FastAccess service and NMS will RMA.

[There may be some exceptions to this. These exceptions are still to be identified]

4. Is a change from Consumer to Business FastAccess allowed? If so, is this on a Change order?

It could be a change order or an N order and D order. These orders will have a CRO FID followed by an order number in the unfielded section of the Header. NMS must RMA if a CRO FID is present.

[This resolution is dependent on COUs who determine how to handle these cases]

5. How does a customer change their Tier of service? Can this be done on a Change order? How does customer change tier of service and from consumer to business?

Yes on a C order.

[This resolution is dependent on COUs who determine how to handle these cases]

6. For services which go through the Service Gateway, are the list of customer required NSPs provided? Is the gateway connectivity checked at the time of taking the SO?

Gateway connectivity to the requested NSP needs to be checked at the time of SO issue.

[However, these procedures are not firmed up yet]

7. We need SO exhibits of each type of FastAccess SO for Category 1 and 2 that will be sent to NMS, such as:
   - New (N) Service Order
   - Disconnect (D) Order
   - Cancellation of a service order
   - Update (correction) to a service order
   - Record Order
   - Change (C) Orders:
     - add or delete FastAccess service
     - deny/restore
     - change FastAccess Service Category/Tier
     - Change NSP
     - Change Circuit ID (?)

[Preliminary examples available only and are subject to changes.

12.1.3 Open Issues

1. On COSMOS assigned orders, we need to have a /TEC FID for the CLLI of the Office Equipment (DSLAM) included in the assignment section of the service order in order to uniquely identify a DSLAM (understand this is not available in COSMOS, key is the NPA/NXX . Will need to determine how we can key on this).

No, CLLI will be on the service order that supports COSMOS assignment. Need to determine if the NPA/NXX can be used as a key in NMS.

12-4

2. Is there a filler after the SO #, Suffix?

Open.

3. When a SO is canceled, are the first 3 characters of the SO# replaced with 3 asterisks?

Can we assume an ORD FID is created followed by the order number in the unfielded section of the Header?

Open for discussion.

4. Will disconnect orders for POTS and FastAccess have an "O" action in the Assignment section?

O action will be used for all equipment that need to come out (including DSLAM ports).

R-DSLAM ports will be represented by PG or DPG cable assignments. *It is unknown what the assignment section will look like for D orders and C orders.*

Handling of facility assignments on D orders for R-DSLAMs is still open.

5. What will a change order for a deny (suspend) or restore look like. In what section will the FIDs be that support this action and what is the name of each FID? Can a deny/restore apply only to FastAccess?

Open.

6. On Business SOs that don't go through the gateway, the physical Circuit ID is required for the NSP, is there a FID to identify this circuit? If so, what section will it be in?

Open.

7. How does the "Quick Service" offering impact ADSL?

Quick Service N orders pass through SOCS and if the ADSL FID is present, these will come to NMS. this might require a D order.

This issue is still Open and is subject to further discussion by the team.

12.2 Service Order Management Issues

- The implications of processing record orders on the flow for pending order processing needs to be evaluated, particularly on the number of orders to be kept.
- How long should disconnect orders be retained? Should completion status be retained?
- How to determine the CO or site locations from the service order. NPA/NXX may need to be used.
- Processing of Business classes of services are to-be-defined.
- Format and FIDS associated with a change order for restoration and denial of service are to-be-defined.
- Should NMS verify that a NSP is accessable from a Service Gateway?

12.3 Network Creation Issues

Other (non-service order) Concerns

- The NMS user will need a copy of the engineering work order for the installation of DSLAM equipment either in a Central Office environment or in a remote site location. NMS needs the CLLI of the equipment, physical location (aisle, bay, relay rack), any connectivity to the DSLAM, NT port assignment, LT card assignments.
- The NMS user will need to receive any assignment changes that are made due to trouble resolutions, so that the NMS database can be updated to reflect the correct assignment for a customer (e.g., a bad pair is the trouble, and the customer is re-assigned to a different pair).
- Does NISC need to have real time access to DSLAM inventory?

12.4 PVC Management Issues

- Alcatel profile names and corresponding numbers are to-be-defined.
- Ascend ATM VPC and VCC attributes and values to be set are to-be-defined.

12.5 NMS External Interfaces Issues

- Response times for commands are currently unknown.

13. Acknowledgments

The authors would like to acknowledge substantial contributions to these requirements by Joan Teer and William Watkins of the PCU. Joan and William were instrumental in the success of this project. They attended several review sessions and provided the critical user needs to the requirement process. Also substantial discussions with Craig Cook on LFACS and Sheri O'Dell on Service Orders are greatly appreciated and acknowledged.

The authors would also like to acknowledge substantial discussions and feedback from the S&T Development Group. Many hours of work with this group helped to substantially improve and refine these requirements. The authors would like to particularly thank Ward Chewning, Fari Behi, Hanif Merali, Ra-Ed Kayyali, Martin Cooper, Miri Iskac, and Sandeep Chawla.

Finally, the authors would also like to acknowledge support and funding for this project from the PCU management, in particular, Jim Johnson, Ken Hawkins, Chris Noll, and Alan White.

13-2

Glossary

AAL5	ATM Adaptation Layer 5
ADSL	Asymetric Digital Subscriber Line
AID	Access Identifier
AIS-LOS	Alarm Indication Signal - Loss Of Signal
API	Applications Programming Interface
ASAM	Asymetric Subscriber Access Multiplexer
ATAG	Autonomously generated correlation Tag
ATM	Asynchronous Tansfer Mode
ATU-C	ADSL Terminating Unit - Central Office
ATU-R	ADSL Terminating Unit - Remote
AWS	Alcatel (ADSL) Work Station
BBOC	Broad Band Operations Center
CCM	Circuit Capacity Management
CEV	Controlled Environmenal Vault
CIDs	Circuit Identifiers
CLLI	COMMON LANGUAGE Location Identifier
CLP	Cell Loss Priority
CMISE	Common Management Information Service Element
CO	Central Office
COSMOS	Computer System for Mainframe Operations
CPUs	Central Processing Units
CSA	Carrier Serving Area/Customer Service Associate
CTAG	Command correlation Tag
DANA	Alcatel's service gateway
DCSC	Data Customers Service Center
DHCP	Dynamic Host Configuration Protocol
DSLAM	Digital Subscriber Line Access Multiplexer
DS1	Digital Signal level 1
DS3	Digital Signal level 3
EOC	Embedded Operations Channel
EMS	Element Management System
FM	Fault Management
GUI	Graphical User Interface

HAL	Hands-off Assignment Logic
HEC	Header Error Control
ID	Identifier
IP	Internet Protocol
IPA	Internet Protocol Address
ISP	Internet Service Provider
LAN	Local Area Network
LATA	Local Access and Transport Area
LCD	Loss of Cell Delineation
LFACS	Loop Facility Assignment and Control System
LIM	Line Interface Module (LT card)
LPF	Low-Pass Filter
LPORT	Logical Port
LT	Line Terminal
MIB	Management Information Base
M&Ps	Method & Procedures
NE	Network Element
NMA	Network Monitoring and Analysis
NMS	Network Management System
NRC	Network Reliability Center
NSDB	Network Services DataBase
NSP	Network Service Provider
NT	Network Terminal
OAM	Operation And Maintenance
OC3	Optical Carrier level 3
OC12	Optical Carrier level 12
OC48	Optical Carrier level 48
OSMINE	Operation Systems Management Integrated Network Elements
OSs	Operation Systems
OTP	Operations Technical Plan
PC/DNA	Personal Computer/Data Network Architecture
PDU	Protocol Data Unit
PM	Performance Management
POI	Point Of Interface
POP	Point Of Presence
POTS	Plain Old Telephone Service
PPORT	Physical Port

PVC	Permanent Virtual Connection
QoS	Quality of Service
RFI	Remote Failure Indicator
RFP	Request For Product
RMA	Request for Manual Assistance
RPEC	Regional Provisioning Engineering Center
SME	Subject Matter Expert
SG	Service Gateway
SID	Source Identifier
SMF	Service Management Function
SNMP	Simple Network Management Protocol
SO	Service Order
SOCS	Service Order Control System
SONET	Synchronous Optical NETwork
TCA	Threshold Crossing Alert
TID	Target IDentifier
TL1	Transaction Language 1
TN	Telephone Number
UBR	Unspecified Bit Rate
UNI	User Network Interface
UPC/NPC	Usage Parameter Control/Network Parameter Control
USOC	Uniform Service Order Code
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VCL	Virtual Channel Link
VPC	Virtual Path Connection
VPI	Virtual Path Identifier
VPL	Virtual Path Link
WORD	Work Order Record and Details

References

1. BellSouth PC/DNA Operations Technical Plan (OTP)- Phase 1, Final Draft,

2. ADSL R2.3 TL1 command Interface Specification, Alcatel Telecom,

3. Ascend Communications, Provisioning Server User's Guide. Ascend Communications, Product Code 80023, Revision 1,

4. Ascend Communications, Fault Server User's Guide, Product Code 80041, Revision

5. Ascend Communications, Fault Server Functional Specification, Document # 020-00006-43, Revision 1.0.4,

6. Ascend Communications, Ascend Enterprise MIB Definition, Product Code 80015, Revision 02,

7. Steve Farkouh, PC/DNA Proposed NetExpert Object Model, OSI,

8. PC/DNA Market Trial DCSC Interaction Methods and Procedures, Version 2.0. Draft Document, BellSouth

9. A1000 ADSL Product Information Release 2.3. Preliminary Document, Alcatel,

10. Fari Behi, Hanif Merali, and Ra-Ed Kayyali, "ADSL NMS GUI Screen Flow," Draft,

11. Alan White, "Proposed Service Definition - FastAccess ADSL,"